Matemática discreta y algebra lineal.pdf

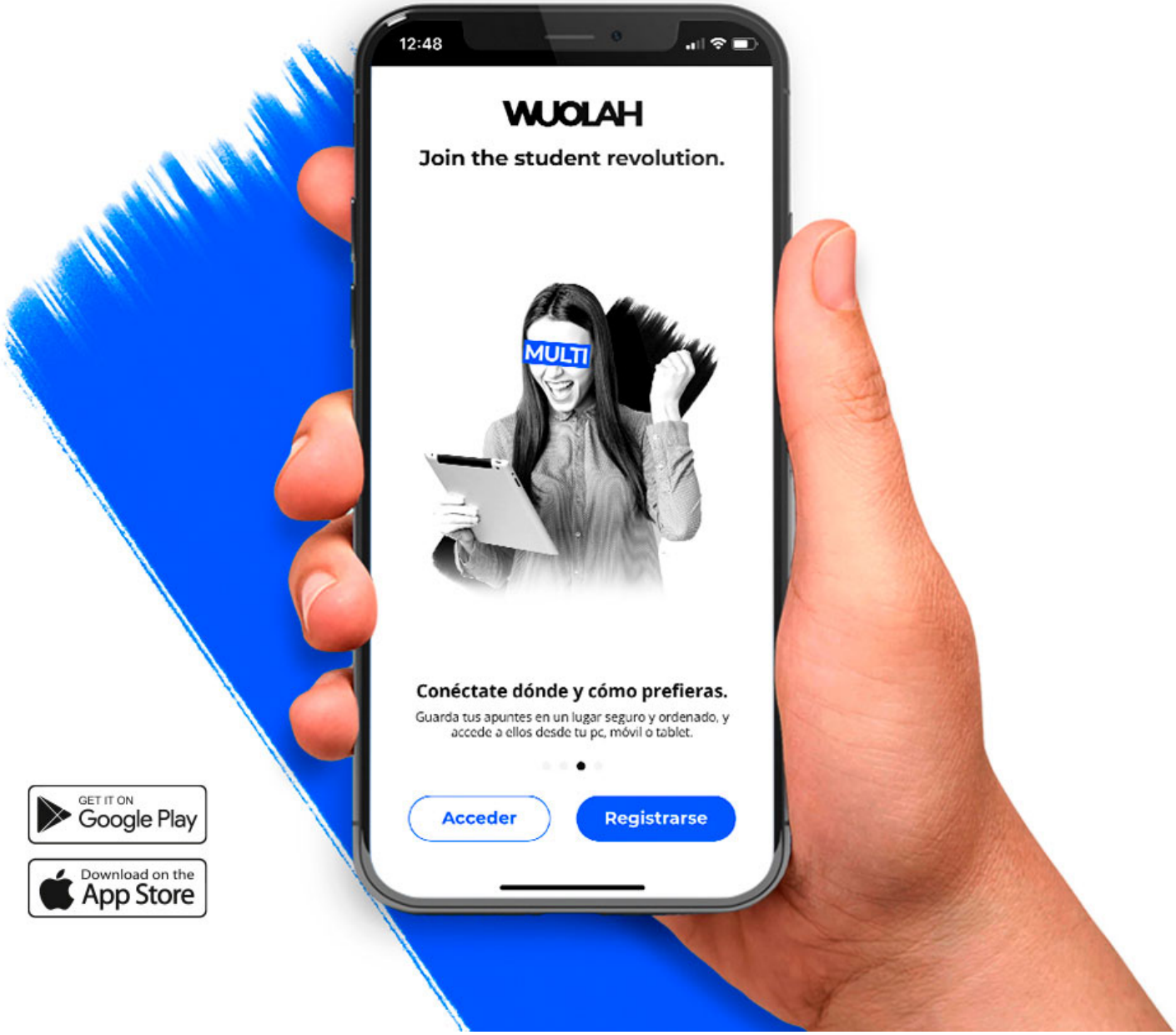
Miranda - Matema?tica Discreta y A?lgebra Lineal

1° Álgebra Lineal y Estructuras Matemáticas

Grado en Ingeniería Informática

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación
Universidad de Granada

Exámenes, preguntas, apuntes.



GET IT ON Google Play

Download on the App Store

Matemática Discreta y Álgebra Lineal

María Burgos Navarro

Jesús García Miranda

Pedro A. García Sánchez

José Carlos Rosales

Departamento de Análisis Matemático, Universidad de Granada

Departamento de Álgebra, Universidad de Granada

Estas notas se han realizado durante la ejecución del proyecto de innovación docente
"Recursos TIC en la docencia matemática, interactividad con la pizarra digital"
de la Universidad de Almería

La mayor parte de los contenidos de estos apuntes han sido extraídos de los apuntes
Notas de Álgebra Lineal y Estructuras Matemáticas
y de las notas del curso
Matemática Discreta.

Índice general

Capítulo 1

Conjuntos, relaciones de equivalencia y aplicaciones

Contenidos de este capítulo

1. Conjuntos

La idea de conjunto es una de las más significativas en Matemáticas. La mayor parte de los conceptos matemáticos están construidos a partir de conjuntos. (Existe una aproximación funcional basada en el λ-cálculo y la Lógica Combinatoria, que hoy en día han tenido una papel fundamental en la programación funcional.)

Podríamos decir que un conjunto es simplemente una colección de objetos a los que llamaremos elementos del conjunto. Esta definición nos bastará para los contenidos de este curso, pero desde el punto de vista matemático es imprecisa y da lugar rápidamente a paradojas. Desde comienzos del siglo XX esta definición dejó de utilizarse por los problemas que acarrea. Por desgracia, dar una definición precisa está bastante lejos de los objetivos de este guión.

- Cuando x sea un elemento de un conjunto A, escribiremos $x \in A$, que se lee "x pertenece a A".
- Diremos que un conjunto A es subconjunto del conjunto B, y lo denotaremos por $A \subseteq B$, si todo elemento de A pertenece a B.
- Un conjunto A es igual que otro conjunto B si tienen los mismos elementos, a saber, si $A \subseteq B$ y $B \subseteq A$. Cuando esto ocurre, escribiremos $A = B$.
- Admitiremos la existencia de un conjunto sin elementos, al que denotemos por $\emptyset$ y llamaremos conjunto vacío.

2. Operaciones con conjuntos

Sean A y B conjuntos.

1) La intersección de A y B es el conjunto formado por los elementos comunes de A y de B, y lo denotamos así
$$A \cap B = \{x \text{ tales que } x \in A \text{ y } x \in B\}.$$
2) La unión de A y B es el conjunto formado al tomar todos los elementos de A y los de B.
$$A \cup B = \{x \text{ tales que } x \in A \text{ o } x \in B\}.$$
3) La diferencia de A y B es el conjunto que tiene por elementos los elementos de A que no están en B.
$$A \setminus B = \{x \in A \text{ tales que } x \notin B\}$$
(siempre que tachemos un símbolo, estamos indicando que no se cumple la condición sin tachar; así $x \notin B$ significa que x no pertenece a B, $A \neq B$ significa que A es distinto de B, etcétera).

4) $\mathcal{P}(A) = \{X \text{ tales que } X \subseteq A\}$ es el conjunto de partes de A o conjunto potencia de A.
5) El producto cartesiano de A y B es el conjunto de parejas cuya primera componente está en A y la sengunda en B. Esto se escribe de la siguiente forma.

$$A \times B = \{(a, b) \text{ tales que } a \in A \text{ y } b \in B\}.$$

Al conjunto $A \times \overset{n}{\cdots} \times A$ lo denotaremos por A^n, para n un entero positivo.

El cardinal de un conjunto es el número de elementos que contiene. Usaremos $\sharp A$ para denotar el cardinal del conjunto A.

- $\sharp\mathcal{P}(A) = 2^{\sharp A}$.
- $\sharp(A \times B) = \sharp A \cdot \sharp B$.

maxima 1: Los conjuntos en `maxima` se pueden definir usando llaves o bien la función `set`.

```
(%i1) {a,a,b,c};
```

(%o1) $\{a, b, c\}$

Definamos un par de conjuntos y veamos cómo se pueden hacer las operaciones hasta ahora descritas con ellos.

```
(%i2) A:{1,2,3,4};
```

(%o2) $\{1, 2, 3, 4\}$

```
(%i3) B:set(3,4,5);
```

(%o3) $\{3, 4, 5\}$

```
(%i4) elementp(5,A);
```

(%o4) false

```
(%i5) elementp(1,A);
```

(%o5) true

```
(%i6) is (A=B);
```

(%o6) false

```
(%i7) is (A=A);
```

(%o7) true

```
(%i8) setequalp(A,B);
```

(%o8) false

```
(%i9) subsetp(A,B);
```

(%o9) false

```
(%i10) subsetp(A,union(A,B));
```

(%o10) true

```
(%i11) intersection(A,B);
```

(%o11) $\{3, 4\}$

```
(%i12) union(A,B);
```

(%o12) $\{1, 2, 3, 4, 5\}$

```
(%i13) setdifference(A,B);
```

(%o13) $\{1,2\}$

```
(%i14) powerset(B);
```

(%o14) $\{\{\},\{3\},\{3,4\},\{3,4,5\},\{3,5\},\{4\},\{4,5\},\{5\}\}$

Nótese que el conjunto vacío se denota por {}.

```
(%i15) is(cardinality(powerset(A))=2^(cardinality(A)));
```

(%o15) true

```
(%i16) cartesian_product(A,B);
```

(%o16) $\{[1,3],[1,4],[1,5],[2,3],[2,4],[2,5],[3,3],[3,4],[3,5],[4,3],[4,4],[4,5]\}$

Podemos además elegir los elementos de A que son impares.

```
(%i17) subset(A,oddp);
```

(%o17) $\{1,3\}$

O bien las sumas de los pares del producto cartesiano con A y B.

```
(%i18) makeset(a+b, [a,b], cartesian_product(A,B));
```

(%o18) $\{4,5,6,7,8,9\}$

maxima 2: Pongamos un ejemplo de una función cuyos argumentos sean conjuntos. Podemos definir la diferencia simétrica de dos conjuntos A y B como $(A \setminus B) \cup (B \setminus A)$.

```
(%i1) A:{1,2,3,4};
```

(%o1) $\{1,2,3,4\}$

```
(%i2) B:set(3,4,5);
```

(%o2) $\{3,4,5\}$

```
(%i3) dif_sim(X,Y):=union(setdifference(X,Y),setdifference(Y,X))$
```

Para definir funciones usamos := en vez de : . El "$" al final de una línea inhibe la salida.

```
(%i4) dif_sim(A,B);
```

(%o4) $\{1,2,5\}$

maxima 3: Podemos definir conjuntos utilizando listas y viceversa, lo cual hace que podamos usar las funciones específicas para listas en conjuntos. Además se pueden definir subconjuntos utilizando funciones booleanas, tal y como vemos a continuación.

```
(%i1) l:makelist(i,i,1,100)$ A:setify(l)$
```

Crea un conjunto con los los enteros del uno al cien.

```
(%i3) B:subset(A,primep);
```

(%o3) $\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97\}$

Escojo aquellos que son primos.

```
(%i4) C:subset(B,lambda([x],is(x>80)));
```

(%o4) $\{83, 89, 97\}$

De entre ellos me quedo con los mayores de 80, que equivale a hacer lo siguiente (ahorrándome la definición de `f`, usando para ello `lambda`, que define de forma anónima una función).

```
(%i5) f(x):=is(x>80)$
(%i6) D:subset(B,f);
```

(%o6) $\{83, 89, 97\}$

3. Relaciones de equivalencia

Sea A un conjunto. Una relación binaria en A es un subconjunto R de $A \times A$. Cuando $(x, y) \in R$ escribimos $x\ R\ y$ y decimos que x está relacionado (mediante R) con y.

Una relación binaria R sobre un conjunto A es una relación de equivalencia si verifica las siguientes propiedades.

1) Para todo $a \in A$, $a\ R\ a$ (R es reflexiva).
2) Dados $a, b \in A$, si $a\ R\ b$, entonces $b\ R\ a$ (R es simétrica).
3) Para cualesquiera $a, b, c \in A$, si $a\ R\ b$ y $b\ R\ c$, entonces $a\ R\ c$ (R es transitiva).

Si R es una relación de equivalencia sobre un conjunto A, y a es un elemento de A, entonces la clase de a es el conjunto de todos los elementos de A que están relacionados con a,

$$[a] = \{x \in A \text{ tales que } x\ R\ a\}.$$

Se define el conjunto cociente de A por R como el conjunto de todas las clases de equivalencia de elementos de A, y se denota por A/R. Así

$$\frac{A}{R} = \{[a] \text{ tales que } a \in A\}.$$

Ejercicio 1: En el conjunto $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ de los números enteros, definimos la siguiente relación de equivalencia.

$$x\ R\ y \text{ si } x - y \text{ es múltiplo de } 5.$$

a) Demuestra que R es una relación de equivalencia.
b) Calcula $[2]$.
c) Describe el conjunto cociente $\frac{\mathbb{Z}}{R}$.
d) ¿Qué cardinal tiene $\frac{\mathbb{Z}}{R}$?

Ejercicio 2: En el conjunto $\mathcal{P}(\{1, 2, 3\})$, definimos la siguiente relación binaria.

$$A \sim B \text{ si } \#A = \#B.$$

a) Demuestra que $\sim$ es una relación de equivalencia.
b) Calcula $[\{1, 2\}]$.
c) Describe el conjunto cociente $\frac{\mathcal{P}(\{1,2,3\})}{\sim}$.
d) ¿Cuántos elementos tiene dicho conjunto cociente?

Dado un conjunto X, una partición de X es una familia de subconjuntos de X, $\{A_i\}_{i \in I}$ ($= \{A_i \text{ tales que } i \in I\}$), de forma que

1) $A_i \neq \emptyset$ para todo $i \in I$,
2) $A_i \cap A_j = \emptyset$ para cualesquiera $i, j \in I$ con $i \neq j$,

3) $X = \bigcup_{i\in I} A_i$ (la unión de todos los elementos de la familia $\{A_i\}_{i\in I}$).
   - Se puede comprobar fácilmente que el hecho de ser R una relación de equivalencia sobre A hace que A/R sea una partición de A.

maxima 4: Veamos cómo se pueden calcular las clases de equivalencia del conjunto $A = \{1,\dots,10\}$ sobre la relación de equivalencia $x\ R\ y$ si $x-y$ es un múltiplo de 3.

Primero definimos el conjunto $\{1,\dots,10\}$. Para ello hacemos una lista con los elementos del uno al diez, y luego la convertimos en conjunto.

```
(%i1) l:makelist(i,i,1,10);
```

$$(\%o1)\qquad [1,2,3,4,5,6,7,8,9,10]$$

```
(%i2) s:setify(l);
```

$$(\%o2)\qquad \{1,2,3,4,5,6,7,8,9,10\}$$

```
(%i3) equiv_classes(s,lambda([x,y],is(remainder(x-y,3)=0)));
```

$$(\%o3)\qquad \{\{1,4,7,10\},\{2,5,8\},\{3,6,9\}\}$$

También podríamos haber definido R, y luego calculado A/R.

```
(%i4) R(x,y):=is(remainder(x-y,3)=0);
```

$$(\%o4)\qquad R(x,y) := \mathrm{is}(\mathrm{remainder}(x-y,3)=0)$$

```
(%i5) equiv_classes(A,R);
```

$$(\%o5)\qquad \{\{1,4,7,10\},\{2,5,8\},\{3,6,9\}\}$$

Se ve que es una partición de A, pues todos sus elementos son no vacíos, disjuntos dos a dos, y la unión de ellos da A.

4. Aplicaciones entre conjuntos

Sean A y B dos conjuntos. Una aplicación f de A en B, que denotaremos como $f : A \to B$, es una correspondencia que a cada elemento de A le asocia un único elemento de B (de nuevo esta definición es algo imprecisa, pero suficiente para nuestro curso). Si $a \in A$, al elemento que le asocia f en B lo denotamos por $f(a)$, y se llama la imagen de a por f. Los conjuntos A y B son el dominio y codominio de f, respectivamente. Llamaremos conjunto imagen de f a

$$\mathrm{Im}(f) = \{f(a) \text{ tales que } a \in A\}.$$

Ejercicio 3: Sea $\mathbb{Q}$ el conjunto de los números racionales y $\mathbb{R}$ el de los reales. ¿Tiene sentido decir que $f : \mathbb{Q} \to \mathbb{R}, x \mapsto \frac{x+1}{x-1}$ es una aplicación?

Si $f : A \to B$ es una aplicación, diremos que f es

1) inyectiva si $f(a) = f(a')$ para $a, a' \in A$, implica $a = a'$;
2) sobreyectiva si $\mathrm{Im}(f) = B$ (para todo $b \in B$, existe $a \in A$ tal que $f(a) = b$);
3) biyectiva si es inyectiva y sobreyectiva.

Ejercicio 4: Demuestra que la aplicación $f : \mathbb{Q} \to \mathbb{R}$ definida por $f(x) = \frac{1}{2}(2x+1)$ es inyectiva pero no sobreyectiva.

Sean $f : A \to B$ y $g : B \to C$ dos aplicaciones. La aplicación composición de f y g (también conocida como f compuesta con g) es la aplicación $g \circ f : A \to C$, definida como $(g \circ f)(a) = g(f(a))$. Para calcular la imagen de un elemento por la composición primero aplicamos f y luego g.

Ejercicio 5: Sean $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$, y $g : \mathbb{Z} \to \mathbb{Q}$, $y \mapsto \frac{1}{2}(y+1)$. Calcula $g \circ f$.

- La composición de aplicaciones es asociativa $(f \circ (g \circ h) = (f \circ g) \circ h)$ pero no es conmutativa ($f \circ g$ no tiene por qué ser igual a $g \circ f$).

maxima 5: Veamos como las funciones cuadrado y sumar uno no conmutan al componerlas.

```
(%i1) f(x):=x^2$ g(x):=x+1$
(%i2) f(g(1)); g(f(1));
```

(%o2) 4

(%o3) 2

```
(%i4) f(g(x))=g(f(x));
```

(%o4) $(x+1)^2 = x^2+1$

```
(%i5) expand(%);
```

(%o5) $x^2+2x+1 = x^2+1$

Sea A un conjunto. La aplicación identidad en A es la aplicación $1_A : A \to A$ definida como $1_A(a) = a$ para todo $a \in A$.

Dada una aplicación $f : A \to B$, decimos que es

1) invertible por la izquierda si existe $g : B \to A$ tal que $g \circ f = 1_A$;
2) invertible por la derecha si existe $g : B \to A$ de forma que $f \circ g = 1_B$;
3) invertible si es invertible a izquierda y a derecha.

- Una aplicación es invertible por la izquierda si y sólo si es inyectiva.
- Una aplicación es invertible por la derecha si y sólo si es sobreyectiva.
- Por tanto, una aplicación es invertible si y sólo si es biyectiva.

Ejercicio 6: Sea $\mathbb{N}$ el conjunto de enteros no negativos. Demuestra que la aplicación $f : \mathbb{N} \to \mathbb{N}$, definida por $f(x) = x^2$ es invertible por la izquierda, pero no por la derecha.

Una aplicación biyectiva f tiene una única inversa que lo es por la derecha y por la izquierda. Dicha aplicación diremos que es la inversa de f y lo denotaremos por f^{-1}.

Ejercicio 7: Demuestra que la aplicación $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = \frac{1}{3}(2x+1)$ es biyectiva. Calcula f^{-1}.

maxima 6: Veamos que la inversa de la función $f(x) = x+1$ (suponemos que el dominio y codominio son los números enteros) es $g(x) = x-1$.

```
(%i1) f(x):=x+1$ g(x):=x-1$
(%i3) f(g(x)); g(f(x));
```

(%o3) x

(%o4) x

Capítulo 2

Técnicas de Conteo

Contenidos de este capítulo

1. Métodos elementales de conteo

Principio de la suma. Sean A_1 y A_2 dos conjuntos disjuntos (es decir, $A_1 \cap A_2 = \emptyset$). Entonces $|A_1 \cup A_2| = |A_1| + |A_2|$.

El principio puede extenderse a tres o más conjuntos.

- Si $A_1, A_2, \cdots, A_n$ son conjuntos disjuntos dos a dos (es decir, $A_i \cap A_j = \emptyset$ para $i \neq j$) entonces

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

El principio de la suma podría enunciarse también como sigue:

- *Si una primera tarea se puede realizar de n_1 formas, y una segunda tarea se puede realizar de n_2 formas, y las dos tareas son incompatibles, entonces hay $n_1 + n_2$ formas de realizar una de las dos tareas.*

Este principio de la suma es muy restrictivo, pues requiere que los conjuntos sean disjuntos, o que las tareas sean incompatibles. Sin embargo, en general, la situación es que los conjuntos no sean disjuntos. En este caso se tiene:

Principio de inclusión-exclusión para dos conjuntos. Sean A_1 y A_2 dos conjuntos. Entonces $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

La idea de este resultado está clara. Si queremos contar los elementos que están en $A_1 \cup A_2$, contamos por una parte los que están en A_1 y por otra parte los que están en A_2, lo que nos da $|A_1| + |A_2|$. Sin embargo, los que se encuentran en $A_1 \cap A_2$ los hemos contado dos veces, luego hemos de restar $|A_1 \cap A_2|$ a la suma anterior.

maxima 7: Vamos a determinar, cuantos números entre 1 y 100 son, bien divisibles por 2, bien divisibles por 3.

Sean A_1 y A_2 los números que son múltiplos de 2 y 3 respectivamente. A_1 tiene cincuenta elementos (desde $2 \cdot 1$ hasta $2 \cdot 50$), mientras que A_3 tiene 33 (desde $3 \cdot 1$ hasta $3 \cdot 33$). Por otra parte, $A_1 \cap A_2$ son los múltiplos de 6, luego tiene 16 elementos (desde $6 \cdot 1$ hasta $6 \cdot 16$). Por tanto

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 50 + 33 - 16 = 67$$

```
(%i1)  a:setify(makelist(i,i,1,100))$
```

```
(%i2)  a1:subset(a,lambda([x],is(mod(x,2)=0)));
```
(%o2) {2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100}

```
(%i3)  a2:subset(a,lambda([x],is(mod(x,3)=0)));
```
(%o3) {3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96, 99}

```
(%i4)  is(length(union(a1,a2))=length(a1)+length(a2)-length(intersection(a1,a2)));
```
(%o4) true

Principio de inclusión-exclusión. Sean $A_1, A_2, \cdots, A_n$ conjuntos. Entonces:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}| + \cdots$$
$$+ (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

maxima 8: Vamos a ver cuantos números entre 1 y 111 son compuestos (lo que nos dará inmediatamente cuántos números primos hay menores que 111).

Dado que $\sqrt{111} < 11$, se tiene que si un número menor o igual que 111 es compuesto, tiene un divisor primo menor que 11. Por tanto, será múltiplo de 2, múltiplo de 3, múltiplo de 5 o múltiplo de 7.

```
(%i1)  a:setify(makelist(i,i,1,111))$
(%i2)  A1:subset(a,lambda([x],is(mod(x,2)=0)))$ a1:length(A1);
```
(%o3) 55

```
(%i4)  A2:subset(a,lambda([x],is(mod(x,3)=0)))$ a2:length(A2);
```
(%o5) 37

```
(%i6)  A3:subset(a,lambda([x],is(mod(x,5)=0)))$ a3:length(A3);
```
(%o7) 22

```
(%i8)  A4:subset(a,lambda([x],is(mod(x,7)=0)))$ a4:length(A4);
```
(%o9) 15

```
(%i10) a12:length(subset(a,lambda([x],is(mod(x,2*3)=0))));
```
(%o10) 18

```
(%i11) a13:length(subset(a,lambda([x],is(mod(x,2*5)=0))));
```
(%o11) 11

Ahora vamos con las intersecciones dos a dos. Al cardinal de $A_i \cap A_j$ lo llamamos a_{ij}.

```
(%i12) a14:length(subset(a,lambda([x],is(mod(x,2*7)=0))));
```
(%o12) 7

```
(%i13) a23:length(subset(a,lambda([x],is(mod(x,3*5)=0))));
```
(%o13) 7

```
(%i14) a24:length(subset(a,lambda([x],is(mod(x,3*7)=0))));
```
(%o14) 5

```
(%i15) a34:length(subset(a,lambda([x],is(mod(x,7*5)=0))));
(%o15) 3
```

Luego calculamos los cardinales de las intersecciones de tres en tres.

```
(%i16) a123:length(subset(a,lambda([x],is(mod(x,2*3*5)=0))));
(%o16) 3

(%i17) a124:length(subset(a,lambda([x],is(mod(x,2*3*7)=0))));
(%o17) 2

(%i18) a134:length(subset(a,lambda([x],is(mod(x,2*5*7)=0))));
(%o18) 1

(%i19) a234:length(subset(a,lambda([x],is(mod(x,3*7*5)=0))));
(%o19) 1
```

Y por último la intersección de todos.

```
(%i20) a1234:length(subset(a,lambda([x],is(mod(x,2*3*5*7)=0))));
(%o20) 0

(%i21) is(length(union(A1,A2,A3,A4))=
       a1+a2+a3+a4-a12-a13-a14-a23-a24-a34+a123+a124+a134+a234-a1234 );
(%o21) true
```

Es decir, entre 1 y 111 hay 81 números compuestos, de donde deducimos que hay 29 números primos (el 1 no es ni primo ni compuesto).

```
(%i22) length(subset(a,primep));
(%o22) 29
```

Principio del producto. Sean A_1, A_2 dos conjuntos. Entonces, $|A_1 \times A_2| = |A_1| \cdot |A_2|$.

Este principio puede generalizarse a tres o más conjuntos, teniéndose en dicho caso:

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdots |A_m|$$

El principio del producto podría enunciarse también como sigue:

- *Si una tarea podemos dividirla en dos (o más) tareas consecutivas, de forma que hay* n_1 *formas de realizar la primera tarea, y* n_2 *formas de realizar la segunda tarea, entonces hay* $n_1 n_2$ *formas de completar la tarea.*

Ejercicio 8: En el sistema de matriculación vigente cada matrícula se compone de cuatro dígitos y tres consonantes en $\mathcal{C} = \{B, C, D, F, G, H, J, K, L, M, N, P, Q, R, S, T, V, W, X, Y, Z\}$. Calcula el número de posibles matriculas.

Ejercicio 9: Calcula cuantos números de 6 cifras, escritos en binario, contienen la secuencia 00 (pista: usa el principio de inclusión-exclusión, teniendo en cuanta que los número que se piden pueden tener una de las formas siguientes, 100___, 1_00__, 1__00_, 1___00).

Número de aplicaciones entre dos conjuntos. Sean A y B dos conjuntos finitos. Entonces el número de aplicaciones de A en B es $|B|^{|A|}$.

Notación: En ocasiones se representa al conjunto de aplicaciones de A en B como B^A, es decir:

$$B^A = \{f : A \to B;\ f \text{ es aplicación}\}$$

Con esta notación se tiene que $\left|B^A\right| = |B|^{|A|}$.

Número de aplicaciones inyectivas. Sea A un conjunto con m elementos y B un conjunto con n elementos. El número de aplicaciones inyectivas de A en B es $n(n-1)\cdots(n-m+1)$.

Variaciones.

1. Se llaman *variaciones con repetición* de n elementos, tomados de m en m a cada una de las posibles elecciones de m elementos, dentro de un conjunto de n elementos, pudiéndose tomar elementos repetidos. Dos posibles elecciones se diferencian, bien en la naturaleza de los elementos elegidos, bien en el orden en que se han elegido.
2. Se llaman *variaciones sin repetición* de n elementos, tomados de m en m a cada una de las posibles elecciones de m elementos, dentro de un conjunto de n elementos, no pudiendo aparecer un elemento más de una vez. Dos posibles elecciones se diferencian, bien en la naturaleza de los elementos elegidos, bien en el orden en que se han elegido.

El número de variaciones con repetición de n elementos, tomados de m en m es igual a n^m. El número de variaciones sin repetición de n elementos, tomados de m en m es $n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}$.

maxima 9: Para hacer una quiniela, debemos elegir una lista de 14 elementos entre los elementos de un conjunto con 3 (1, X, 2). Son por tanto, variaciones con repetición de 3 elementos tomados de 14 en 14. El número total de posibles apuestas es

```
(%i1)  3^12;
(%o1)  531441
```

maxima 10: En una carrera participan 35 personas. El ganador recibe una medalla de oro, el segundo clasificado una medalla de plata y el tercer clasificado una medalla de bronce.

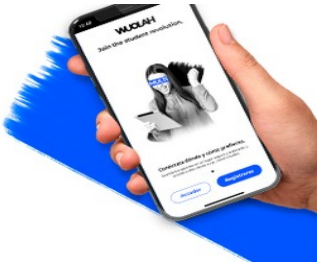
El número de formas diferentes en que se pueden repartir las medallas corresponde al número de variaciones sin repetición de 35 elementos, tomados de 3 en 3. Por tanto es $35 \cdot 34 \cdot 33 = 39270$.

Para usar las funciones de combinatoria tenemos que cargar el paquete `functs`.

```
(%i2)  load(functs)$
(%i3)  permutation(35,3);
(%o3)  39270
```

El principio del palomar. Si queremos repartir n objetos en m cajas, y $n > m$ entonces al menos una caja ha de contener 2 o más objetos.

Nótese que repartir objetos en cajas es equivalente a definir una aplicación del conjunto de objetos en el conjunto de las cajas (la imagen de un elemento nos dice en que caja se coloca). Decir que una caja tiene dos o más objetos se traduce en que la aplicación no es inyectiva (pues esos dos elementos tendrían la misma imagen). El principio del palomar se enunciaría entonces:



- *Si* $n > m$ *no existen aplicaciones inyectivas de un conjunto de cardinal* n *en un conjunto de cardinal* m.

Si tenemos un grupo de 500 personas (bastaría con tener 367) debe haber dos que celebren el cumpleaños el mismo día (siempre y cuando todas celebren su cumpleaños).

En este caso las cajas serían cada uno de los días del año, mientras que los objetos a repartir son las personas.

Ejercicio 10: Demuestra que dado un conjunto formado por n números enteros, $\{x_1, x_2, \cdots, x_n\}$, podemos encontrar un subconjunto suyo cuya suma sea múltiplo de n (pista: considera los enteros $y_i = x_1 + \cdots + x_i$, $i \in \{1, \ldots, n\}$ y toma sus restos de dividir por n).

Principio del palomar generalizado. Si queremos repartir n objetos en m cajas, al menos una caja ha de contener al menos n/m elementos.

Obviamente, si n/m no es entero, se toma el número entero inmediatamente superior.

2. Combinaciones

En secciones anteriores estudiamos como, de un conjunto de n elementos podíamos extraer m, de forma que el orden en que se extraían los elementos fuera significativo. En esta trataremos de encontrar como extraer m elementos de un conjunto que tiene n, pero ahora no importa el orden en que se elijan, sino únicamente la naturaleza de estos elementos.

En términos de conjuntos, nos preguntamos cuántos subconjuntos de cardinal m tiene un conjunto con n elementos. Vamos a denotar por $\binom{n}{m}$ a tal cantidad.

Es fácil ver que $\binom{n}{0} = 1$, pues cada conjunto de cardinal n tiene un único subconjunto con 0 elementos, a saber, el conjunto vacío. De la misma forma se tiene que $\binom{n}{n} = 1$ (pues el único subconjunto de cardinal n de un conjunto de n elementos es el propio conjunto).

También es fácil ver que $\binom{n}{m} = \binom{n}{n-m}$ pues cada subconjunto de m elementos determina de forma única un subconjunto de $n - m$ elementos (concretamente, el de los elementos que no pertenecen a él) y viceversa.

Por último, una tercera propiedad referente a estos números nos dice que $\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$.

Número de combinaciones. Sean $m, n \in \mathbb{N}$ con $m \leq n$. Entonces

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

maxima 11: El número de subconjuntos con 2 elementos del conjunto $\{a, b, c, d, e\}$ es

```
(%i1)  binomial(5,2);
(%o1)  10

(%i2)  subset(powerset({a,b,c,d,e}),lambda([x],is(length(x)=2)));
(%o2)  {a, b}, {a, c}, {a, d}, {a, e}, {b, c}, {b, d}, {b, e}, {c, d}, {c, e}, {d, e}

(%i3)  length(%);
(%o3)  10
```

Ejercicio 11: Demuestra que el número de cadenas de n bits que contienen exactamente m unos (y por tanto $n - m$ ceros) es $\binom{n}{m}$.

Sabemos que si X es un conjunto con n elementos, entonces X tiene 2^n subconjuntos (las álgebras de Boole $\mathbb{B}^n$ y $\mathcal{P}(X)$ son isomorfas). Deducimos entonces que, para cualquier $n \in \mathbb{N}$ se verifica que

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$

maxima 12: Supongamos que un departamento está formado por 7 mujeres y 9 hombres, y se quiere formar una comisión con cinco miembros, de forma que haya al menos un hombre y una mujer en la comisión. Determinemos cuántas posibles comisiones pueden formarse con esas condiciones.

Para esto, vemos en primer lugar que pueden formarse

```
(%i1)  binomial(16,5);
(%o1)  4368
```

posibles comisiones con 5 miembros.

De ellas,

```
(%i2)  binomial(9,5);
(%o2)  126
```

no contienen ninguna mujer (están formadas únicamente por hombres), mientras que

```
(%i3)  binomial(7,5);
(%o3)  21
```

no contienen ningún hombre. Por tanto, como el número que buscamos es el complentario de aqullas que no tienen ni hombres ni mujeres, y estos conjuntos son disjuntos, el número posible de comisiones es $4368 - (126 + 21) = 4221$.

Teorema del Binomio. Sea A un anillo conmutativo, y $a, b \in A$. Entonces, para cualquier $n \in \mathbb{N}$ se verifica que:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n$$

maxima 13: El coeficiente de $a^7 b^3$ en $(a+b)^{10}$ es $\binom{7}{3} = 35$.

```
(%i1)  expand((a+b)^7);
(%o1)  b^7 + 7 a b^6 + 21 a^2 b^5 + 35 a^3 b^4 + 35 a^4 b^3 + 21 a^5 b^2 + 7 a^6 b + a^7
```

Usando el teorema del binomio se tiene que:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = (1+1)^n = 2^n$$

algo que ya habíamos obtenido anteriormente.

Hasta ahora hemos estudiado, como de un conjunto de n elementos podemos elegir m, sin que influya el orden en que se pueden elegir los elementos, y sin que puedan repetirse los elementos. Es lo que se llama *combinaciones (sin repetición) de n elementos tomados de m en m*. Nos planteamos a continuación el caso en el que los elementos puedan repetirse. Por ejemplo, tenemos en una caja bolas rojas, negras y blancas, y extraemos 4 bolas. ¿Cuántas extracciones distintas podemos realizar?

Se trata, de un conjunto de tres elementos ($\{R, N, B\}$) elegir cuatro, pudiéndose repetir los elementos, y sin que influya el orden en que los elegimos. Da igual la extracción RNBN que RNNB. Lo único que importa es que se han elegido una bola roja, dos bolas negras y una blanca.

En este caso, las posibles extracciones son (suponemos que tenemos al menos cuatro bolas de cada color):

RRRR RRRN RRRB RRNN RRNB RRBB RNNN RNNB

RNBB RBBB NNNN NNNB NNBB NBBB BBBB

es decir, un total de 15.

Para encontrar una forma de generalizar esto, vamos a escribir las quince posibles extracciones como sigue:

RRRRxx RRRxNx RRRxxB RRxNNx RRxNxB RRxxBB RxNNNx RxNNxB

RxNxBB RxxBBB xNNNNx xNNNxB xNNxBB xNxBBB xxBBBB

y vemos que cada extracción está determinada por la posición que ocupan las dos x en la cadena _____ El número de posiciones que quedan a la izquierda de las dos equis nos indican la cantidad de bolas rojas; el número de posiciones que quedan entre las dos equis nos indican el número de bolas negras mientras que el número de posiciones a la derecha de las dos equis nos indican la cantidad de bolas blancas. Así, colocando las equis en las posiciones 2 y 4 nos queda _x_x__, lo que nos da una bola roja, una bola negra y dos bolas blancas.

Puesto que entre las seis posiciones podemos colocar las dos equis de $\binom{6}{2} = 15$ formas diferentes obtenemos que se pueden hacer un total de 15 extracciones diferentes.

Situémonos en el caso general. Supongamos que tenemos un conjunto con n elementos, que podrían ser bolas de n colores diferentes, y extraemos m elementos (se supone que de cada color hay al menos m bolas). Esto es lo que se llama *combinaciones con repetición de* n *elementos tomados de* m *en* m. Para determinar cuantas combinaciones con repetición hay, identificamos cada combinación con la elección de la posición de $m-1$ equis de un total de $n+m-1$ posibles posiciones. El número de combinaciones con repetición de n elementos, tomados de m en m resulta ser entonces $\binom{n+m-1}{m} = \binom{n+m-1}{n-1}$.

maxima 14: Vamos a determinar cuantas soluciones naturales tiene la ecuación $x+y+z+t = 13$. Para resolverlo, planteamos el problema de otra forma. Supongamos que tenemos cuatro tipos de bolas (rojas, negras, blancas y azules), y extraemos trece bolas. Cada extracción la podemos identificar con una solución de la ecuación anterior, donde x es el número de bolas rojas, y es el número de bolas negras, z es el número de bolas blancas y t es el número de bolas azules.

El número de posibles extracciones es el número de combinaciones con repetición de 4 elementos tomados de 13 en 13. Su valor es

```
(%i1)  binomial(16,3);
(%o1)  560
```

Supongamos ahora que queremos resolver la misma ecuación, pero queremos que las variables tomen valores mayores o iguales que 1. En ese caso, llamamos $x' = x-1$, $y' = y-1$, $z' = z-1$, $t' = t-1$, con lo que la ecuación se transforma en $x'+y'+z'+t' = 9$, y están permitidas todas las soluciones naturales. El número de soluciones es

```
(%i3)  binomial(9+4-1,4-1);
(%o3)  220
```

Por tanto, de las 560 soluciones de la ecuación $x+y+z+t=13$ hay 476 $(560-84)$ en las que alguna de las variables toma el valor cero.

Ejercicio 12: Supongamos que tenemos 15 caramelos (iguales) y los queremos repartir entre 5 niños. ¿De cuántas formas podemos hacerlo?

Ejercicio 13: Consideremos las variables x, y y z. Un monomio en esas tres variables es una expresión de la forma $x^a y^b z^c$, con a, b, c números naturales. El grado del monomio $x^a y^b z^c$ es $a+b+c$. Calcula cuántos monomios hay de grado 10 en las variables x, y y z.

3. Permutaciones

En esta sección estudiaremos las formas diferentes de ordenar los elementos de un conjunto. Dado un conjunto X con n elementos, una *permutación* en X es una ordenación de los elementos de X. Otra forma de definir una permutación en X es como una aplicación biyectiva $X \to X$.

maxima 15: Por ejemplo, si $X=\{1,2,3\}$, hay seis permutaciones en X que se corresponden con las seis formas de ordenar los elementos de X.

```
(%i1)  permutations([1,2,3]);
(%o1)  [1,2,3], [1,3,2], [2,1,3], [2,3,1], [3,1,2], [3,2,1]
```

En general, si X es un conjunto con n elementos, el número de permutaciones en X es igual al número de aplicaciones inyectivas $X \to X$, pues toda aplicación inyectiva $X \to X$ es biyectiva. Este número fue calculado en la sección dedicada a las variaciones, y sabemos que vale $n\cdot(n-1)\cdots 2\cdot 1 = n!$.

Algo más complicado es ordenar los elementos de un conjunto cuando alguno de sus elementos aparece repetido.

maxima 16: Por ejemplo, nos preguntamos de cuántas formas podemos ordenar las letras de la palabra *cara*.

```
(%i1)  permutations([c,a,r,a]);
(%o1)  {[a, a, c, r], [a, a, r, c], [a, c, a, r], [a, c, r, a], [a, r, a, c], [a, r, c, a],
[c, a, a, r], [c, a, r, a], [c, r, a, a], [r, a, a, c], [r, a, c, a], [r, c, a, a]}

(%i2)  length(%);
(%o2)  12
```

Para llegar a este resultado, supongamos que distinguimos las dos aes que aparecen en la palabra, escribiendo una de ellas en negrita, y realizamos las 24 ordenaciones posibles.

```
(%i3)  permutations([c,a1,r,a2]);
(%o3)  {[a1, a2, c, r], [a1, a2, r, c], [a1, c, a2, r], [a1, c, r, a2], [a1, r, a2, c], [a1, r, c, a2], [a2, a1, c, r],
[a2, a1, r, c], [a2, c, a1, r], [a2, c, r, a1], [a2, r, a1, c], [a2, r, c, a1], [c, a1, a2, r], [c, a1, r, a2],
[c, a2, a1, r], [c, a2, r, a1], [c, r, a1, a2], [c, r, a2, a1], [r, a1, a2, c], [r, a1, c, a2], [r, a2, a1, c],
[r, a2, c, a1], [r, c, a1, a2], [r, c, a2, a1]}
```

Vemos que cada 2 ordenaciones de las letras de car**a** da lugar a la misma ordenación de las letras de cara (la que resulta de intercambiar "a" con "**a**"). Por tanto, las letras de cara se pueden ordenar de $\frac{24}{2}=12$ formas distintas.

Otra forma de razonar este resultado es como sigue:

Para ordenar las letras de *cara*, situamos en primer lugar las dos "aes". Esto podemos hacerlo de $\binom{4}{2}$ formas diferentes. Una vez situadas las dos "aes", colocamos la "c", para la que tenemos dos posibilidades. Por tanto, hay $\binom{4}{2} \cdot 2 = 12$ formas diferentes de colocarla. La posición de la "r" queda determinada por la de la "c" y las "aes".

Ejercicio 14: Estudia de cuántas formas podemos ordenar las letras de la palabra "rara".

Proposición. Supongamos que tenemos una lista de n objetos, de r tipos diferentes. Del tipo 1 hay un total de n_1 objetos, todos ellos indistinguibles. Del tipo 2 hay n_2 objetos, y así hasta el tipo r, del que hay n_r objetos. Entonces el número total de ordenaciones de estos objetos es

$$\frac{n!}{n_1!n_2!\cdots n_r!}$$

Este problema es equivalente al de repartir objetos distinguibles en cajas distinguibles. Supongamos que tenemos n objetos, y queremos repartirlos en r cajas, de forma que en la primera caja haya n_1 objetos, en la segunda carta haya n_2 objetos, y así, hasta la r-ésima caja, en la que debe haber n_r objetos.

Los n_1 objetos que van a la primera caja se pueden elegir de $\binom{n}{n_1}$ formas. Nos quedan entonces $n - n_1$ objetos, y de estos elegimos n_2 para la segunda caja, lo cual podemos hacerlo de $\binom{n-n_1}{n_2}$ formas. Repitiendo el razonamiento, y usando el principio del producto llegamos a que las formas distintas en que podemos repartir los objetos en las cajas es

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-\cdots-n_{r-1}}{n_r} = \frac{n!}{n_1!n_2!\cdots n_r!}$$

Se deja como ejercicio encontrar una biyección entre las distintas ordenaciones de n objetos donde r tipos de objetos, y del tipo k-ésimo hay n_k objetos, y las distribuciones de n objetos distinguibles en r cajas distinguibles, de forma que en la caja k-ésima haya n_k-objetos.

Coeficiente multinomial. Sea $n \in \mathbb{N}$, y $n_1, n_2, \cdots, n_r \in \mathbb{N}$ tales que $n_1 + n_2 + \cdots + n_r = n$. Se define el coeficiente multinomial $\binom{n}{n_1\ n_2\ \cdots\ n_r}$ como

$$\binom{n}{n_1\ n_2\ \cdots\ n_r} = \frac{n!}{n_1!n_2!\cdots n_r!}$$

En el caso $r = 2$ se tiene que $\binom{n}{n_1\ n_2} = \binom{n}{n_1} = \binom{n}{n_2}$. En este caso se denominan *coeficientes binomiales*.

maxima 17: Tenemos cuatro jugadores, y repartimos cinco cartas a cada uno de una baraja de 40 cartas. Vamos a calcular de cuantas formas distintas se pueden repartir. Para esto, consideramos las cartas como las bolas, a las que hay que distribuir en 5 cajas: 4 por cada uno de los jugadores, y una quinta por las 20 cartas que quedan sin repartir.

Se trata entonces de distribuir 40 objetos distinguibles en cinco cajas también distinguibles, de forma que en las cuatro primeras haya 5 objetos y en la última haya 20. El número de formas de hacerlo es

```
(%i1)  40!/(5!*5!*5!*5!*20!);
(%o1)  161731817508852759168 0
(%i2)  multinomial(40,[5,5,5,20]);
(%o2)  161731817508852759168 0
```

Teorema Multinomial. Sea A un anillo conmutativo, y $x_1, x_2, \cdots x_r \in A$. Entonces, para cada $n \in \mathbb{N}$ se verifica que:

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{n_1+n_2+\cdots+n_r=n} \binom{n}{n_1\ n_2\ \cdots\ n_r} x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}.$$

maxima 18: El número 3 se puede expresar de $\binom{3+3-1}{3-1} = 10$ formas diferentes como suma de 3 números naturales. Éstas corresponden con los exponentes de las variables en el desarrollo de $(x+y+z)^3$.

```
(%i1)  expand((x+y+z)^3);
(%o1)  z^3+3*y*z^2+3*x*z^2+3*y^2*z+6*x*y*z+3*x^2*z+y^3+3*x*y^2+3*x^2*y+x^3
```

El teorema multinomial tiene también una demostración combinatoria.

$$(x_1 + x_2 + \cdots + x_r)^n = \underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_1} \underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_2} \cdots \underbrace{(x_1 + x_2 + \cdots + x_r)}_{c_n}$$

Cada término de $(x_1+x_2+\cdots+x_r)^n$ se obtiene multiplicando un sumando de c_1, con un sumando de c_2 y así hasta c_n. El coeficiente de $x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}$ en $(x_1 + x_2 + \cdots + x_r)^n$ se obtendrá contando cuantos términos (obtenidos como acabamos de decir) hay en los que ha elegido n_1 veces el sumando x_1, n_2 veces el sumando x_2 y así sucesivamente.

En definitiva, lo que hay que hacer es ver de cuantas maneras diferentes se pueden distribuir los "objetos" $c_1, c_2, \cdots, c_n$ en r cajas distinguibles $(x_1, x_2, \cdots, x_r)$; y esto sabemos que se puede hacer de $\binom{n}{n_1\ n_2\ \cdots\ n_r}$ formas diferentes.

Capítulo 3

Aritmética entera y modular

Contenidos de este capítulo

1. Principio de inducción y recurrencia

1.1. Principio de inducción. Si A es un subconjunto de $\mathbb{N}$ tal que:
$0 \in A$
Si $n \in A$ entonces $n+1 \in A$
Entonces $A = \mathbb{N}$.

Este principio es la base de muchas demostraciones en las que intervienen los números naturales. Veamos un ejemplo.

maxima 19: Vamos a demostrar que para todo $n \in \mathbb{N}$ se verifica que

$$2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$$

Para esto, consideramos el conjunto A cuyos elementos son los números naturales para los que se verifica la propiedad anterior, es decir,

$$A = \{n \in \mathbb{N} : 2^0 + \cdots + 2^n = 2^{n+1} - 1\}$$

Claramente se tiene que $0 \in A$, pues $2^0 = 2^{0+1} - 1$.
Supongamos ahora que $n \in A$, y veamos que $n+1 \in A$, es decir, supongamos que $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$ y comprobemos que $2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1$.

$$2^0 + 2^1 + \cdots + 2^n + 2^{n+1} = (2^0 + 2^1 + \cdots + 2^n) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

Por el principio de inducción se tiene que $A = \mathbb{N}$, es decir, la propiedad es cierta para todo $n \in \mathbb{N}$.

```
(%i1)  simpsum:false;
(%o1)  false
(%i2)  sum(2^i,i,0,n);
(%o2)  sum(2^i, i, 0, n)
```

```
(%i3)  simpsum:true;
(%o3)  true

(%i4)  sum(2^i,i,0,n);
(%o4)  2^(n+1)-1
```

Una demostración basada en el principio de inducción es lo que se conoce como una demostración por inducción.

Si queremos demostrar por inducción que $P(n)$ es cierto para todo $n \in \mathbb{N}$ (donde $P(n)$ es una propiedad que hace referencia a n), hemos de realizar dos pasos:

- Paso 1: Demostramos que $P(0)$ es cierto.
- Paso 2: Demostramos que si $P(n)$ es cierto, entonces también es cierto $P(n+1)$.

La suposición de que $P(n)$ es cierto es lo que se conoce como *hipótesis de inducción*.

Si quisiéramos demostrar que $P(n)$ es cierto para todo $n \geq k$, el primer paso deberá ser demostrar que $P(k)$ es cierto, mientras que el segundo no variaría.

maxima 20: Demuestra que para todo $n \geq 1$ se verifica que

$$1+2+\cdots+n = \frac{n(n+1)}{2}$$

Hacemos esto por inducción:

- Paso 1: Para $n = 1$ el resultado es trivialmente cierto.
- Paso 2: La hipótesis de inducción es que $1+2+\cdots+n = \frac{n(n+1)}{2}$. A partir de ella hemos de probar que $1+2+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2}$

$$(1+2+\cdots+n)+n+1 = \frac{n(n+1)}{2}+n+1 = \frac{n(n+1)}{2}+\frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

```
(%i5)  sum(i,i,1,n);
(%o5)  (n^2+n)/2
```

El principio de inducción nos dice que si A es un subconjunto de $\mathbb{N}$ que satisface las dos siguientes propiedades:

- $0 \in A$
- $n \in A \Longrightarrow n+1 \in A$

Entonces $A = \mathbb{N}$. Este axioma puede leerse de la forma siguiente:

> Si A es un subconjunto de $\mathbb{N}$ que es distinto de $\mathbb{N}$, entonces, o $0 \notin A$, o existe $n \in \mathbb{N}$ tal que $n \in A$ y $n+1 \notin A$.

Esta formulación del principio de inducción (equivalente a la vista anteriormente) nos permite demostrar una propiedad importante de los números naturales.

Principio de buena ordenación. Sea A un subconjunto de $\mathbb{N}$ distinto del conjunto vacío. Entonces A tiene mínimo.

Se dice que m es el mínimo de A si $m \in A$ y $m \leq n$ para todo $n \in A$.

Hasta ahora hemos usado el principio de inducción para demostrar propiedades referentes a los números naturales. Veamos ahora como definir funciones con dominio en $\mathbb{N}$.

Sucesiones. Sea X un conjunto. Una sucesión en X es una aplicación $x : \mathbb{N} \to X$.
Si $x : \mathbb{N} \to X$ es una sucesión, denotaremos normalmente al elemento $x(n)$ como x_n.

A la hora de definir una sucesión en X, podemos optar, bien por definir explícitamente el valor de x_n para todo $n \in \mathbb{N}$, o bien, definir el valor de x_0, y a partir de x_n definir lo que vale x_{n+1}. El principio de inducción nos asegura que de esta forma se define una función $x : \mathbb{N} \to X$ (aunque formalizar esto es bastante engorroso, la idea consiste en considerar A el subconjunto de los números naturales n para los que x_n está definido. Claramente, $0 \in A$ y si $n \in A$ entonces $n+1 \in A$, luego $A = \mathbb{N}$).

Esta forma de definir sucesiones se llama recursiva, pues para obtener el valor de x_n necesitamos el valor de x_{n-1}, que a su vez necesita el valor de x_{n-2}, y así, hasta x_0. Es decir, la sucesión recurre a la propia sucesión para obtener un valor determinado.

maxima 21: Dado $a \in \mathbb{R}^*$, definimos la sucesión x_n como sigue:

- $x_0 = 1$
- $x_{n+1} = a \cdot x_n$

Es fácil comprobar que $x_n = a^n$.

```
(%i1)  load(solve_rec)$
(%i2)  solve_rec(x[n]=x[n-1]*a,x[n],x[0]=1);
```
(%o2) $x_n = a^n$

maxima 22: Definimos la sucesión $x_n = 2^{n+1} - 1$. En este caso hemos dado explícitamente x_n para cada $n \in \mathbb{N}$.

Definimos ahora y_n como sigue:

$$y_0 = 1$$
$$y_{n+1} = y_n + 2^{n+1}$$

Que ha sido definida de forma recursiva.

Ya hemos visto anteriormente que $x_n = y_n$ para todo $n \in \mathbb{N}$.

```
(%i3)  solve_rec(y[n]=y[n-1]+2^n,y[n],y[0]=1);
```
(%o3) $y_n = 2^{n+1} - 1$

maxima 23: La sucesión $x_n = 1 + 2 + \cdots + n$ puede ser definida recursivamente como:

$$x_1 = 1 \qquad x_{n+1} = x_n + n + 1$$

También se podría comenzar con $x_0 = 0$.

Ya hemos visto que $x_n = \frac{n(n+1)}{2}$.

```
(%i4)  solve_rec(x[n]=x[n-1]+n,x[n],x[0]=0);
```
(%o4) $x_n = \dfrac{n\,(n+1)}{2}$

Podemos definir $n!$ de forma recursiva:

1. $0! = 1$
2. $(n+1)! = (n+1) \cdot n!$

Ejercicio 15: Sea $m \in \mathbb{N}$. Definimos la sucesión:

$$x_0 = 0 \qquad x_{n+1} = x_n + m.$$

Demuestra que $x_n = m \cdot n$ (hágase; así vemos cómo definir el producto de números naturales a partir de la suma).

maxima 24: Consideremos ahora la sucesión dada por

$$f_0 = 1 \quad f_1 = 1 \qquad f_n = f_{n-1} + f_{n-2}$$

Es fácil calcular los primeros términos de esta sucesión:

$f_2 = 1+1 = 2$; $f_3 = 1+2 = 3$; $f_4 = 2+3 = 5$; $f_5 = 3+5 = 8$

y así sucesivamente. Parece claro que está bien definido el valor de f_n para cualquier $n \in \mathbb{N}$. Sin embargo, esta definición no se ajusta al método de recurrencia dado anteriormente (pues en este caso, para calcular un término es necesario recurrir a los dos términos anteriores, mientras que en el método dado anteriormente, únicamente necesitamos conocer el término anterior). Para subsanar este problema, veamos un nuevo principio de inducción.

```
(%i5)  solve_rec(f[n]=f[n-1]+f[n-2],f[n],f[0]=0,f[1]=1);
```

$$(\%o5) \quad f_n = \frac{\left(\sqrt{5}+1\right)^n}{\sqrt{5}\,2^n} - \frac{\left(\sqrt{5}-1\right)^n (-1)^n}{\sqrt{5}\,2^n}$$

Segundo principio de inducción. Sea A un subconjunto de $\mathbb{N}$. Supongamos que se verifica:

1. $0 \in A$.
2. Para cualquier n, $\{0, 1 \cdots n-1\} \subseteq A \Longrightarrow n \in A$

Entonces $A = \mathbb{N}$.

Formalmente, la primera condición no es necesaria, pues para $n = 0$ la segunda condición afirma $\emptyset \subseteq A \Longrightarrow 0 \in A$, y puesto que la primera parte es siempre cierta ($\emptyset \subseteq A$), la condición 2 implica que $0 \in A$. Sin embargo, en la práctica suele ser necesario comprobar que $0 \in A$.

Notemos también que si la condición 1 se cambia por una de la forma $0, 1, \ldots, k \in A$, la tesis del teorema sigue siendo cierta.

Este segundo principio puede usarse, tanto para definir sucesiones como para probar propiedades de los números naturales.

maxima 25: Sea x_n la sucesión definida mediante

$$x_0 = 1 \qquad x_{n+1} = \sum_{k=0}^{n} x_k$$

Calculemos una fórmula general para x_n. Para esto, hallemos los primeros términos:

$x_0 = 1$; $x_1 = x_0 = 1$; $x_2 = x_0 + x_1 = 1+1 = 2$; $x_3 = 1+1+2$; $x_4 = 1+1+2+4 = 8$; $x_5 = 1+1+2+4+8 = 16$.

Parece ser que x_n responde a la expresión

$$x_n = \begin{cases} 1 & \text{si} \quad n = 0 \\ 2^{n-1} & \text{si} \quad n \geq 1 \end{cases}$$

Comprobémosla por inducción, utilizando el segundo principio

- Paso 1: El resultado es cierto para $n = 0$ y $n = 1$.
- Paso 2: La hipótesis de inducción es $x_n = 2^{n-1}$

A partir de esto tenemos que $x_{n+1} = 1+1+2+\cdots+2^{n-1} = 1+(1+2+\cdots+2^{n-1}) = 1+2^n-1 = 2^n$, como queríamos.

En esta demostración se ha sustituido $(1+2+\cdots+2^{n-1})$ por 2^n-1, algo que ya hemos visto con anterioridad.

Podemos comprobar que realizar esta demostración usando el primer principio de inducción no es posible. Nuestra hipótesis de inducción sería que $x_n = 2^{n-1}$, y a partir de ella, tendríamos que demostrar que $x_{n+1} = 2^n$. Sin embargo, lo único que podemos hacer es

$$x_{n+1} = x_0 + x_1 + \cdots + x_{n-1} + x_n = x_0 + x_1 + \cdots + x_{n-1} + 2^{n-1}$$

y puesto que nuestra hipótesis no nos dice nada del valor de x_{n-1}, x_{n-2}, etc., no podemos concluir que $x_{n+1} = 2^n$.

Si intentamos hacer esto con maxima directamente, nos encontramos con un problema.

```
(%i1)  load(solve_rec)$
(%i2)  solve_rec(x[n]=sum(x[i],i,0,n-1),x[n],x[0]=1);
apply: found u evaluates to 1 where a function was expected.
#0: lambda([u],[-u[1],u[2]])(u=1)(solve_rec.mac line 510)
#1: get_exps(expr=-'sum(x[i],i,0,n-1),var=n)
#2: solve_rec_lin_cc(coeffs=[1],ihom=-'sum(x[i],i,0,n-1), %f=x, %n=n,cond=[x[0] = 1])(solve_rec.mac
line 391) – an error. To debug this try: debugmode(true);
```

Sin embargo, podemos usar que $x_{n+1} - x_n = x_n$.

```
(%i3)  solve_rec(x[n+1]-x[n]=x[n],x[n],x[1]=1);
(%o3)  x_n = 2^(n-1)
```

2. Los números enteros

Dado un entero z, $-z$ es su opuesto, y denotamos por $|z| = \text{máx}\{z, -z\}$ al valor absoluto de z.

Propiedades de la suma. La suma de enteros es

- asociativa,
- tiene elemento neutro (el cero sumado a cualquier elemento da de nuevo ese elemento),
- todo elemento tiene inverso (si sumamos un entero con su opuesto obtenemos el cero),
- conmutativa,
- cancelativa ($a+b = a+c$ implica $b = c$; esto es consecuencia inmediata de la existencia de elemento inverso).

El conjunto de los números enteros con la suma es por tanto un grupo abeliano.

Propiedades del producto. El producto de números enteros es

- conmmutativo,
- asociativo,
- tiene elemento neutro (el uno),
- es cancelativo para elementos no nulos,
- distributivo ($a(b+c) = ab+ac$, que nos permite además sacar factor común).

Así el conjunto de los números enteros es un anillo conmutativo.

Propiedad de la división. Dados $a, b \in \mathbb{Z}$, con $b \neq 0$, existen $q, r \in \mathbb{Z}$ únicos de forma que $a = qb + r$ y $0 \leq r < |b|$.

A q y r los llamaremos cociente y resto de dividir a entre b, y los denotaremos por a div b y a mód b, respectivamente.

Dados a y b enteros, decimos que a divide a b, o que b es un múltiplo de a, si existe $c \in \mathbb{Z}$ tal que $b = ac$. Usaremos $a \mid b$ para denotar que a divide a b.

Ejercicio 16: Sean $a, b, c \in \mathbb{Z}$. Demuestra que si $c \mid a$ y $c \mid b$, entonces para todo $x, y \in \mathbb{Z}$, $c \mid xa + yb$.

Sea $p \in \mathbb{Z} \setminus \{-1, 1\}$ (-1 y 1 son los únicos enteros que tiene inverso para el producto). Decimos que p es irreducible si los únicos enteros que dividen a p son 1, -1, p y $-p$. El entero p es primo si siempre que $p|ab$, para a y b enteros, se tiene que $p|a$ o $p|b$.

- Un entero es primo si y sólo si es irreducible.

Decimos que dos enteros son primos relativos si los únicos enteros que dividen a ambos son 1 y -1. (Nótese que 1 y -1 dividen a cualquier número entero.)

Teorema de Bézout. Sean $a, b \in \mathbb{Z}$. Entonces a y b son primos relativos si y sólo si existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$.

Teorema fundamental de la aritmética. Todo número entero mayor que uno se puede expresar de forma única (salvo reordenaciones) como producto de números primos positivos.

Ejercicio 17: Calcula todos los divisores enteros positivos de 120.

Sean $a, b \in \mathbb{Z}$, con $a \neq 0$ o $b \neq 0$. Un entero d es un máximo común divisor de a y b si

1) $d \mid a$ y $d \mid b$,
2) si $c \mid a$ y $c \mid b$, con c un entero, entonces $c \mid d$.

Análogamente, un entero m es un mínimo común múltiplo de a y b si

1) $a \mid m$ y $b \mid m$,
2) si $a \mid c$ y $b \mid c$, con c un entero, entonces $m \mid c$.

De forma similar se puede definir el máximo común divisor y el mínimo común múltiplo de un conjunto de enteros $\{a_1, \ldots, a_n\}$ con n un entero positivo.

- Si d es un máximo común divisor de a y b, también lo es $-d$, y éstos son los únicos máximos divisores comunes de a y b. Lo mismo ocurre con el mínimo común múltiplo. Esto se debe a que si $a \mid b$, entonces $-a \mid b$. Cuando escribamos $\gcd\{a, b\}$ nos referiremos al máximo común divisor positivo de a y b. Para el mínimo común múltiplo utilizaremos $\operatorname{lcm}(a, b)$.
- Sean $a = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $b = vp_1^{\beta_1} \cdots p_r^{\beta_r}$, con $u, v \in \{1, -1\}$, $p_1, \ldots, p_r$ primos distintos y $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ enteros no negativos (algunos pueden ser cero, pues los primos que aparecen en a no tienen por qué aparecer en b). Entonces

$$\gcd\{a, b\} = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}},$$

$$\operatorname{lcm}\{a, b\} = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}.$$

- $\gcd\{a, b\}\operatorname{lcm}\{a, b\} = |ab|$.

Algoritmo de Euclides.
Entrada: a, b enteros positivos.
Salida: $\gcd\{a, b\}$.

$(a_0, a_1) := (a, b)$.
Mientras $a_1 \neq 0$
$(a_0, a_1) := (a_1, a_0 \text{ mód } a_1)$.
Devuelve a_0.

Ejercicio 18: Calcula el máximo común divisor de 237 y 99.

maxima 26: Veamos algunos ejemplos de cálculo con `maxima`.

```
(%i1) primep(38129);
(%o1)                                false
(%i2) next_prime(38129);
(%o2)                                38149
(%i3) prev_prime(38129);
(%o3)                                38119
(%i4) factor(38129);
(%o4)                             7  13  419
(%i5) 7*13*419;
(%o5)                                38129
(%i6) gcd(15,18);
(%o6)                                 3
(%i7) quotient(101,34);
(%o7)                                 2
(%i8) remainder(101,34);
(%o8)                                 33
(%i9) 2*34+33;
(%o9)                                101
```

Hay que tener cuidado con estas funciones, pues el resto no se define como nosotros lo hemos hecho.

```
(%i10) quotient(-150,17);remainder(-150,17);
(%o10)                               -8
(%o11)                               -14
```

Si queremos un resto y cociente acordes a nuestra definición de división podemos hacer lo siguiente.

```
(%i12) cociente(a,b):=(a-mod(a,b))/b;
```

(%o12) $$\text{cociente}(a,b) := \frac{a - \text{mod}(a,b)}{b}$$

```
(%i13) cociente(-150,17);mod(-150,17);
```

(%o13) -9

(%o14) 3

```
(%i15) is(-8*17+-14=-9*17+3);
```

(%o15) true

3. Ecuaciones diofánticas lineales

Una ecuación diofántica lineal es una expresión de la forma $a_1x_1 + \cdots + a_nx_n = b$, con $a_1, \ldots, a_n, b \in \mathbb{Z}$. Una solución a dicha ecuación es una n-upla $(c_1, \ldots, c_n)$ de elementos enteros de forma que $a_1c_1 + \cdots + a_nc_n = b$.

Teorema de Bézout generalizado. Sea $\{a_1, \ldots, a_n\}$ un conjunto de enteros, y d su máximo común divisor. Entonces existen $u_1, \ldots, u_n \in \mathbb{Z}$ tales que $a_1u_1 + \cdots + a_nu_n = d$.

Así la ecuación diofántica $a_1x_1 + \cdots + a_nx_n = b$ tiene solución si y sólo si $d \mid b$. Las soluciones de $a_1x_1 + \cdots + a_nx_n = b$ son las mismas que las de las ecuación $\frac{a_1}{d}x_1 + \cdots + \frac{a_n}{d}x_n = \frac{b}{d}$.

Para $n = 2$, tenemos ecuaciones en dos variables. Usamos las incógnitas x e y por comodidad. Si x_0, y_0 es una solución particular de $ax+by = c$, con $\gcd\{a,b\} = 1$, entonces todas las soluciones de esa ecuación son de la forma

$$\begin{cases} x = x_0 + bk, \\ y = y_0 - ak, \end{cases}$$

con $k \in \mathbb{Z}$.

Algoritmo extendido de Euclides.
Entrada: a, b enteros positivos.
Salida: $s, t, d \in \mathbb{Z}$ tales que $d = \gcd\{a,b\}$ y $as + bt = d$.

$(a_0, a_1) := (a, b)$.
$(s_0, s_1) := (1, 0)$.
$(t_0, t_1) := (0, 1)$.
Mientras $a_1 \neq 0$
  $q := a_0$ div a_1.
  $(a_0, a_1) := (a_1, a_0 - a_1q)$.
  $(s_0, s_1) := (s_1, s_0 - s_1q)$.
  $(t_0, t_1) := (t_1, t_0 - t_1q)$.
$d := a_0$, $s := s_0$, $t := t_0$.
Devuelve s, t, d.

maxima 27: Resolvamos la ecuación $40x + 15y = 30$. Usando `gcdex` obtenemos lo siguiente.

```
(%i1) gcdex(40,15);
```

(%o1) $[-1, 3, 5]$

Lo que significa que $40 \times (-1) + 15 \times 3 = 5$. Como 5 divide a 30, la ecuación tiene solución. Multiplicamos por 6 ($6 \times 5 = 30$) y obtenemos lo siguiente.

```
(%i2) %*6;
```

$$(\%o2) \qquad [-6, 18, 30]$$

Que equivale a multiplicar la igualdad $40 \times (-1) + 15 \times 3 = 5$ por 6. Por tanto, una solución de nuestra ecuación $30 \times (-6) + 15 \times 18 = 30$.

Nótese que la ecuación $40x + 15y = 30$ es equivalente a $8x + 3y = 6$ (hemos dividido por el máximo común divisor de 40 y 15). Si x_0, y_0 es una solución de dicha ecuación, $x = x_0 + 3k$ e $y = y_0 - 8k$ es una solución de $8x + 3y = 6$ para todo $k \in \mathbb{Z}$.

```
(%i3) gcdex(8,3);
```

$$(\%o3) \qquad [-1, 3, 1]$$

```
(%i4) %*6;
```

$$(\%o4) \qquad [-6, 18, 6]$$

Así todas las soluciones de $40x + 15y = 30$ son

$$\begin{cases} x = -6 + 3k, \\ y = 18 - 8k. \end{cases}$$

maxima 28: Resolvamos ahora la ecuación $121x - 77y = 88$.

```
(%i1)  gcd(121,-77);
```

$$(\%o1) \qquad 11$$

Al dividir por 11, la ecuación queda reducida a $11x - 7y = 8$.

```
(%i2)  l:gcdex(11,-7);
```

$$(\%o2) \qquad [2, 3, 1]$$

```
(%i3)  8*l;
```

$$(\%o3) \qquad [16, 24, 8]$$

Por lo que tenemos que una solución particular es $x_0 = 16$ e $y_0 = 24$. Siendo además todas las soluciones de la forma $x = x_0 - 7k$, $y = y_0 - 11k$ con k un entero cualquiera.

4. Ecuaciones en congruencias de grado uno

Sean $a, b, m \in \mathbb{Z}$. Escribimos $a \equiv b \pmod{m}$, que se lee "a es congruente con b módulo m", para indicar que $m \mid a - b$.

Una ecuación en congruencias de grado uno (o lineal) es una expresión de la forma $ax \equiv b \pmod{m}$. Una solución para dicha ecuación es un entero c de forma que $ac \equiv b \pmod{m}$. Nótese que las soluciones de $ax \equiv b \pmod{m}$ son las posibles x de la ecuación diofántica $ax + my = b$.

- La ecuación $ax \equiv b \pmod{m}$ tiene solución si y sólo si $\gcd\{a, m\} \mid b$.
- Si $d = \gcd\{a, m\}$ y $d \mid b$, entonces las ecuaciones $ax \equiv b \pmod{m}$ y $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ tienen las mismas soluciones.
- Si $\gcd\{a, m\} = 1$, y x_0 es una solución de $ax \equiv b \pmod{m}$, entonces el conjunto de todas las soluciones de la ecuación es $\{x_0 + km$ tales que $k \in \mathbb{Z}\}$.
- La ecuación $ax + c \equiv b \pmod{m}$ tiene las mismas soluciones que la ecuación $ax \equiv b - c \pmod{m}$.
- La ecuación $ax \equiv b \pmod{m}$ tiene las mismas soluciones que la ecuación $(a \bmod m)x \equiv (b \bmod m) \pmod{m}$.

- Si $au + mv = 1$, con $u, v \in \mathbb{Z}$, entonces bu es una solución de $ax \equiv b \pmod{m}$.

maxima 29: Veamos si tiene solución la ecuación $54x \equiv 6 \pmod{34}$, y en caso de tener, vamos a describir su conjunto de soluciones.

```
(%i1) remainder(54,34);
```

$$(\%o1) \qquad 20$$

Al ser 54 mód 34 igual a 20, la ecuación anterior es equivalente a $20x \equiv 6 \pmod{34}$.

```
(%i2) gcd(20,34);
```

$$(\%o2) \qquad 2$$

Como $2|6$, la ecuación tiene solución, y es equivalente a $10x \equiv 3 \pmod{17}$. Usando `gcdex` obtenemos los coeficientes de Bézout para 10 y 17.

```
(%i2) gcdex(10,17);
```

$$(\%o2) \qquad [-5, 3, 1]$$

Lo que viene a decir que $(-5) \times 10 + 3 \times 17 = 1$. Así una solución de $10x \equiv 3 \pmod{17}$ es $(-5)3$, que vale -15. Así todas las soluciones de nuestra ecuación son de la forma $-15 + 17k$ con $k \in \mathbb{Z}$.

Ejercicio 19: Encuentra todas las soluciones enteras de

$$121x \equiv 2 \pmod{196}.$$

maxima 30: Vamos a resolver el sistema

$$\begin{cases} x \equiv 5495 \pmod{7643} \\ x \equiv 7569 \pmod{8765} \end{cases}$$

Por la primera ecuación, sabemos que x es de la forma $x = 5495 + 7643k$ con k un entero cualquiera. Substituimos en la segunda y k se convierte en la nueva incógnita: $5495 + 7643k \equiv 7569 \pmod{8765}$. Como

```
(%i1)  7569-5495;
```

$$(\%o1) \qquad 2074$$

tenemos que resolver $7643k \equiv 2074 \pmod{8765}$. El inverso de 7643 módulo 8765 lo calculamos (de existir) con el algoritmo extendido de Euclides.

```
(%i2)  gcdex(7643,8765);
```

$$(\%o2) \qquad [2617, -2282, 1]$$

Despejamos

```
(%i3)  mod(2617*2074,8765);
```

$$(\%o3) \qquad 2123$$

y obtenemos que $k = 2123 + 8765t$ para cualquier entero t. Substituyendo k en la expresión de x, llegamos a $x = 5495 + 7643(2123 + 8765t)$.

```
(%i4)  expand(5495+7643*(2123+8765*t));
```

$$(\%o4) \qquad 66990895\,t + 16231584$$

Por lo que $x = 66990895t + 16231584$ para todo $t \in \mathbb{Z}$ es una solución del sistema de congruencias. Lo podemos comprobar como sigue.

```
(%i6)  mod(16231584,[7643,8765]);
```
$$(\%o6) \qquad [5495, 7569]$$

Ejercicio 20: Resuelve los siguientes sistemas de congruencias.

$$\left.\begin{array}{ll} 2x \equiv 3 & (\text{mód } 5) \\ 3x \equiv 1 & (\text{mód } 4) \end{array}\right\} \qquad \left.\begin{array}{ll} 2x \equiv 2 & (\text{mód } 4) \\ 6x \equiv 3 & (\text{mód } 9) \\ 2x \equiv 3 & (\text{mód } 5) \end{array}\right\}$$

$$\left.\begin{array}{ll} 2x \equiv 2 & (\text{mód } 4) \\ 3x \equiv 6 & (\text{mód } 12) \end{array}\right\} \qquad \left.\begin{array}{ll} x \equiv 1 & (\text{mód } 2) \\ 3x \equiv 2 & (\text{mód } 6) \\ 5x \equiv 1 & (\text{mód } 7) \end{array}\right\}$$

5. El anillo de los enteros módulo un entero positivo

Dado un entero positivo m, denotamos por $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ (que es el conjunto de restos posibles de la división por m), y por eso este conjunto se conoce a veces como el conjunto de los enteros módulo m.

En $\mathbb{Z}_m$ definimos una suma y un producto de la siguiente forma. Dados $a, b \in \mathbb{Z}_m$,

- $a \oplus b = (a + b)$ mód m,
- $a \otimes b = (ab)$ mód m.

Propiedades de la suma. Conmutativa, asociativa, elemento neutro y elemento inverso.

Propiedades del producto. Conmutativa, asociativa, elemento neutro y distributiva.

- Un elemento $a \in \mathbb{Z}_m$ tiene inverso para el producto si y sólo si $\gcd\{a, m\} = 1$. Si $au + mv = 1$, entonces u mód m es el inverso de a en $\mathbb{Z}_m$.

Ejercicio 21: Calcula el inverso para el producto de 121 en $\mathbb{Z}_{196}$.

Ejercicio 22: Calcula el resto de dividir 4225^{1000} entre 7.

Ejercicio 23: Prueba que dado un número entero m o bien se verifica que $m^2 \equiv 0 \pmod 8$, o $m^2 \equiv 1 \pmod 8$, o $m^2 \equiv 4 \pmod 8$.

maxima 31: Escribamos una función para calcular $\mathbb{Z}_m$, para m un entero positivo.

```
(%i1) Z(m):=setify(makelist(i,i,0,m-1));
```
$$(\%o1) \qquad Z(m) := \text{setify}(\text{makelist}(i, i, 0, m-1))$$
```
(%i2) Z(10);
```
$$(\%o2) \qquad \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
```
(%i3) tieneinverso(x,m):=is(gcd(x,m)=1);
```

```
(%o3)  tieneinverso(x,m) := is(gcd(x,m)=1)
```

El inverso lo podemos calcular con la función `inv_mod`.

```
(%i4) inv_mod(3,10);
(%o4)  7
(%i5) inv_mod(2,10);
(%o5)  false
```

Veamos los elementos que tienen inverso en $\mathbb{Z}_{12}$.

```
(%i6) subset(Z(12),lambda([x],tieneinverso(x,12)));
(%o6)  1,5,7,11
```

Como 11 es primo, todo elemento no nulo de $\mathbb{Z}_{11}$ tiene inverso:

```
(%i7) every(lambda([x],tieneinverso(x,11)),disjoin(0,Z(11)));
(%o7)  true
```

Por último, resolvamos la ecuación $137x \equiv 26 \pmod{155}$, que es equivalente a resolver la ecuación $137x = 26$ en $\mathbb{Z}_{155}$.

```
(%i9)  inv_mod(137,155);
(%o9)  43
(%i10) mod(43*26,155);
(%o10)  33
```

Capítulo 4

Retículos y álgebras de Boole

Contenidos de este capítulo

1. Conjuntos ordenados.

Relación de orden. Sea X un conjunto, y $\leq$ una relación binaria en X. Se dice que $\leq$ es una relación de orden si se verifican las siguientes propiedades.

- Reflexiva: $x \leq x$ para todo $x \in X$.
- Antisimétrica: Si $x \leq y$ e $y \leq x$ entonces $x = y$.
- Transitiva: Si $x \leq y$ e $y \leq z$ entonces $x \leq z$.

Si X es un conjunto en el que tenemos definida una relación de orden $\leq$, se dice que $(X, \leq)$ es un conjunto ordenado (o, si está claro cual es la relación $\leq$ se dice simplemente que X es un conjunto ordenado).

Si $\leq$ es una relación de orden en X que satisface la propiedad adicional de que dados $x, y \in X$ entonces $x \leq y$ ó $y \leq x$, se dice entonces que $\leq$ es una relación de orden total, y que $(X, \leq)$ (o X) es un conjunto totalmente ordenado (en ocasiones, para destacar que $(X, \leq)$ es una relación de orden, pero que no es total se dice que $\leq$ es una relación de orden parcial y que $(X, \leq)$ es un conjunto parcialmente ordenado).

Ejercicio 24:

1. El conjunto de los números naturales, con el orden natural ($m \leq n$ si existe $k \in \mathbb{N}$ tal que $n = m + k$) es un conjunto totalmente ordenado. De la misma forma, también lo son $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ y $(\mathbb{R}, \leq)$.
2. Dado un conjunto X, entonces $\mathcal{P}(X)$, con el orden dado por la inclusión es un conjunto ordenado. Prueba que si X tiene más de un elemento, este orden no es total.
3. En el conjunto de los números naturales, la relación de divisibilidad es una relación de orden que no es total. Prueba que, sin embargo, en el conjunto de los números enteros esta relación no es de orden.
4. Para cualquier número natural n consideramos el conjunto

   $$D(n) = \{m \in \mathbb{N} : m|n\}$$

   Entonces $(D(n), |)$ es un conjunto (parcialmente) ordenado.

Sea $(X, \leq)$ es un conjunto ordenado, e Y un subconjunto de X. Definimos en Y el orden $x \preceq y$ si $x \leq y$ (vistos como elementos de X). Entonces, $(Y, \preceq)$ es un conjunto ordenado. De ahora en adelante, el orden en Y lo denotaremos igual que en X.

Si $(X, \leq)$ es un conjunto totalmente ordenado, entonces, para cualquier $Y \subseteq X$ se tiene que $(Y, \leq)$ es un conjunto totalmente ordenado.

La definición de conjunto ordenado puede hacerse también a partir de la noción de *orden estricto*.

Orden estricto. Sea X un conjunto, y $<$ una relación binaria en X. Se dice que $<$ es un orden estricto si se verifican las siguientes propiedades:

: Antirreflexiva Para cualquier $x \in X$ se tiene que $x \not< x$.
: Transitiva Si $x < y$ e $y < z$ entonces $x < z$.

Es fácil comprobar que si $\leq$ es una relación de orden en un conjunto X, entonces si definimos

$$x < y \text{ si } x \leq y \text{ y } x \neq y$$

se tiene que $<$ es una relación de orden estricto en X.

De la misma forma, si $<$ es una relación de orden estricto en X entonces la relación siguiente:

$$x \leq y \text{ si } x < y \text{ o } x = y$$

es una relación de orden en X.

Vemos entonces que los conceptos de *relación de orden* y *relación de orden estricto* son equivalentes, pues dada una relación de orden tenemos determinada una relación de orden estricto y viceversa. Además, los caminos para pasar de orden a orden estricto, y de orden estricto a orden, son uno el inverso del otro.

A continuación vamos a construir un grafo (dirigido) asociado a una relación de orden. Aún cuando los grafos serán estudiados con posterioridad, la representación de una relación de orden mediante este grafo ayuda a visualizar mejor el orden dado.

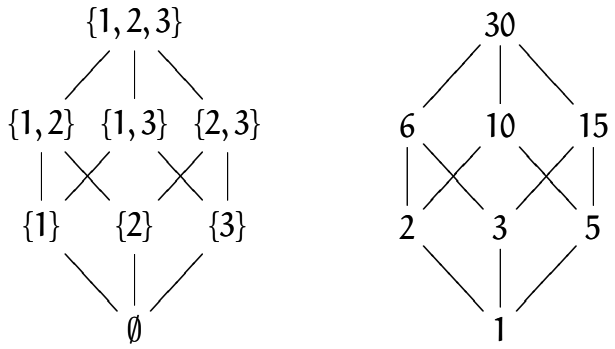
Diagrama de Hasse. El diagrama de Hasse de un conjunto ordenado $(X, \leq)$ es un grafo dirigido cuyos vértices son los elementos de X, y existe un lado de x a y si $x < y$ y no existe z tal que $x < z < y$.

El diagrama de Hasse de un conjunto ordenado está definido para cualquier conjunto ordenado. Sin embargo, en general dicho diagrama no permite recuperar el orden. Por ejemplo, en el caso del conjunto $(\mathbb{R}, \leq)$, dado cualquier $x \in \mathbb{R}$ no existe ningún $y \in \mathbb{R}$ que esté conectado a x por algún lado.

Sin embargo, si el conjunto X es finito, entonces dados $x, y \in X$ se tiene que $x \leq y$ si $x = y$ o existe algún camino que parta de x y termine en y.

Una forma habitual de representar el diagrama de Hasse es dibujar los lados como líneas ascendentes, lo que implica colocar los vértices de forma apropiada.

Vamos a representar los diagramas de Hasse de los conjuntos ordenados $\mathcal{P}(\{1,2,3\})$ y $D(30)$.



Observa como la estructura de conjunto ordenado es igual en ambos casos.

Maximales, minimales, máximo y mínimo. Sea $(X, \leq)$ un conjunto ordenado.

1. Un elemento $x \in X$ se dice que es maximal, si no existe $y \in X$ tal que $x \leq y$ y $x \neq y$.
2. Un elemento $x \in X$ se dice que es máximo, si para todo $y \in X$ se verifica que $y \leq x$.

De la misma forma se puede definir lo que es un elemento minimal y lo que es un mínimo.

Nótese, que si un conjunto tiene máximo, entonces este es único. Además, en el caso de que tenga máximo, entonces tiene sólo un elemento maximal, que coincide con el máximo.

Idéntica observación vale para mínimo y elemento minimal.

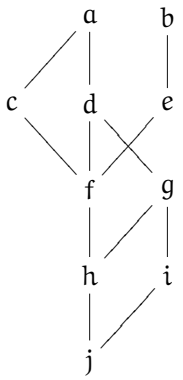
Denotaremos por máx(X) al máximo del conjunto X, en el caso de que exista, y por mín(X) al mínimo.

Cotas superiores, inferiores, supremo e ínfimo. Sea $(X, \leq)$ un conjunto ordenado, e Y un subconjunto de X. Consideramos en Y el orden inducido de X.

1. Un elemento $x \in X$ se dice que es *cota superior* de Y si $x \geq y$ para todo $y \in Y$.
2. Un elemento $x \in X$ se dice que es *supremo* de Y si es el mínimo del conjunto de las cotas superiores de Y.

De la misma forma se define lo que es una cota inferior y un ínfimo.

Ejercicio 25: Sea $X = \{a, b, c, d, e, f, g, h, i, j\}$ con el orden dado por el diagrama de Hasse



e $Y = \{c, d, f, g, h\}$. Calcula

1. el conjunto de las cotas superiores de Y,
2. el supremo de Y en caso de existir,
3. los elementos maximales de Y,
4. el conjunto de las cotas inferiores de Y,
5. su ínfimo (en caso de existir),
6. máximo y mínimo, si es que existen.

Cuando un conjunto tiene supremo éste es único. Podemos entonces hablar de *el supremo de* Y, y lo representaremos mediante sup(Y).

De la misma forma, denotaremos por ínf(Y) al ínfimo del conjunto Y cuando exista.

Cuando un conjunto tiene máximo, entonces también tiene supremo, y coincide con él. En el último ejemplo vemos como el recíproco no es cierto, pues Y tiene supremo pero no tiene máximo.

Cuando el supremo de un conjunto pertenezca al conjunto, entonces será también el máximo.

maxima 32:

```
(%i1)  menores(x,rel,conj):=subset(conj,lambda([y],rel(y,x) ))$
(%i2)  mayores(x,rel,conj):=subset(conj,lambda([y],rel(x,y) ))$
(%i3)  D:setdifference(divisors(30),{1,2,30});
(%o3)  {3,5,6,10,15}

(%i4)  menores(15,lambda([x,y],is(mod(y,x)=0)), {1,2,3,4,5,6,7});
(%o4)  {1,3,5}

(%i5)  minimal(x,rel,con):=is(menores(x,rel,con)={x}) and elementp(x,con)$
(%i6)  maximal(x,rel,con):=is(mayores(x,rel,con)={x}) and elementp(x,con)$
(%i7)  minimal(3,lambda([x,y],is(mod(y,x)=0)), D);
(%o7)  true

(%i8)  minimales(rel,con):=subset(con,lambda([x],minimal(x,rel,con)))$
(%i9)  maximales(rel,con):=subset(con,lambda([x],maximal(x,rel,con)))$
(%i10) div(x,y):=is(mod(y,x)=0)$
(%i11) minimales(div,D);
(%o11)  {3,5}

(%i12) maximales(div,D);
(%o12)  {6,10,15}

(%i13) minimo(rel,con):=block(local(m),
        m:listify(minimales(rel,con)),
       if (is(length(m)=1)) then m[1] else
       error ("Error no hay minimo"))$
(%i14) maximo(rel,con):=block(local(m),
       m:listify(maximales(rel,con)),
       if (is(length(m)=1)) then m[1] else
       error("Error no hay maximo"))$
(%i15) maximo(div,D);
Error no hay maximo
#0: maximo(rel=div,con=3,5,6,10,15) – an error. To debug this try: debugmode(true);

(%i16) minimo(div,D);
Error no hay minimo
#0: minimo(rel=div,con=3,5,6,10,15) – an error. To debug this try: debugmode(true);

(%i17) cotasuperior(x,rel,con):=is(con=menores(x,rel,con))$
(%i18) cotainferior(x,rel,con):=is(con=mayores(x,rel,con))$
(%i19) cotainferior(1,div,D);
(%o19)  true

(%i20) cotassuperiores(rel,con,amb):=subset(amb,lambda([x],cotasuperior(x,rel,con)))$
(%i21) cotasinferiores(rel,con,amb):=subset(amb,lambda([x],cotainferior(x,rel,con)))$
(%i22) cotasinferiores(div,D,divisors(30));
(%o22)  {1}

(%i23) cotasinferiores(div,D,D);
(%o23)  {}
```

```
(%i24) supremo(rel,con,amb):=minimo(rel,cotassuperiores(rel,con,amb))$
(%i25) infimo(rel,con,amb):=maximo(rel,cotasinferiores(rel,con,amb))$
(%i26) supremo(div,D,D);
```
Error no hay minimo
#0: maximo(rel=div,con=)
#1: supremo(rel=div,con=3,5,6,10,15,amb=3,5,6,10,15) – an error. To debug this try: debugmode(true);

```
(%i27) infimo(div,D,divisors(30));
(%o27) 1

(%i28) supremo(div,D,divisors(30));
(%o28) 30
```

Buen orden. Sea $(X, \leq)$ un conjunto ordenado. Se dice que $\leq$ es un buen orden si todo subconjunto no vacío de X tiene mínimo. En tal caso, se dice que $(X, \leq)$ (o X) es un conjunto bien ordenado.

Observación: Todo conjunto bien ordenado es un conjunto totalmente ordenado, pues dados dos elementos $x, y \in X$ el subconjunto $\{x, y\}$ tiene mínimo. Si $\text{mín}(\{x, y\}) = x$ entonces $x \leq y$, mientras que si $\text{mín}(\{x, y\}) = y$ entonces $y \leq x$.

El recíproco no es cierto. Busca un ejemplo.

Ejercicio 26: El conjunto de los números naturales, con el orden usual, es un conjunto bien ordenado.

Orden producto. Sean $(X_1, \leq_1)$ y $(X_2, \leq_2)$ dos conjuntos ordenados.

- Se define el *orden producto* en $X_1 \times X_2$ como sigue:
$$(x_1, x_2) \preceq (y_1, y_2) \text{ } si \text{ } x_1 \leq_1 y_1 \text{ } y \text{ } x_2 \leq_2 y_2.$$
- Se define el *orden lexicográfico* en $X_1 \times X_2$ como sigue:
$$(x_1, x_2) \leq_{lex} (y_1, y_2) \overset{\text{def}}{\iff} \begin{cases} x_1 <_1 y_1 & \acute{o} \\ x_1 = y_1 \text{ } y \text{ } x_2 \leq_2 y_2. \end{cases}$$

Claramente, si $(x_1, x_2) \preceq (y_1, y_2)$ entonces $(x_1, x_2) \leq_{lex} (y_1, y_2)$.

Propiedades del orden producto. Si $(X_1, \leq_1)$ y $(X_2, \leq_2)$ son dos conjuntos ordenados, entonces $(X_1 \times X_2, \preceq)$ y $(X_1 \times X_2, \leq_{lex})$ son conjuntos ordenados.

Además, si $\leq_1$ y $\leq_2$ son órdenes totales (resp. buenos órdenes) entonces $\leq_{lex}$ es un orden total (resp. buen orden).

Observación: Si tenemos n conjuntos ordenados $X_1, X_2, \ldots, X_n$, podemos definir recursivamente el orden producto y el orden lexicográfico en $X_1 \times X_2 \times \cdots \times X_n$.

Supuesto definido el orden producto $\preceq$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:
$$(x_1, \ldots x_{n-1}, x_n) \preceq (y_1, \ldots, y_{n-1}, y_n) \text{ } si \text{ } (x_1, \ldots, x_{n-1}) \preceq (y_1, \ldots, y_{n-1}) \text{ y } x_n \leq y_n,$$
es decir, definimos el orden producto en $(X_1 \times \cdots \times X_{n-1}) \times X_n$.

Supuesto definido el orden lexicográfico $\leq_{lex}$ en $X_1 \times \cdots \times X_{n-1}$ se define en $X_1 \times \cdots \times X_n$:

$$(x_1, \ldots x_{n-1}, x_n) \leq_{lex} (y_1, \ldots, y_{n-1}, y_n) \overset{\text{def}}{\iff} \begin{cases} (x_1, \ldots, x_{n-1}) <_{lex} (y_1, \ldots, y_{n-1}) & \text{ó} \\ (x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1}) \ y \ x_n \leq y_n. \end{cases}$$

Sea el conjunto

$$\mathcal{A} = \{\ , a, b, c, d, e, f, g, h, i, j, l, l, m, n, \tilde{n}, o, p, q, r, s, t, u, v, w, x, y, z\},$$

es decir, las 27 letras del alfabeto junto con el espacio en blanco.

Claramente, $\mathcal{A}$ tiene un orden total de todos conocido.

Supongamos que n es el número de letras de la palabra más larga de la lengua española. Entonces, cada palabra puede representarse como un elemento de $\mathcal{A}^n$ (poniendo tantos espacios al final como sea necesario).

Cuando ordenamos las palabras, tal y como vienen en un diccionario, nos fijamos en la primera letra, y es la que nos da el orden. Cuando ésta coincide, pasamos a la segunda, y es ésta entonces la que nos da el orden. De coincidir también, nos fijamos en la tercera, y así sucesivamente. Es decir, las palabras de la lengua están ordenadas siguiendo el orden lexicográfico.

Ejercicio 27: Consideramos en $\mathbb{N} \times \mathbb{N}$ los órdenes producto ($\leq$) y lexicográfico $\leq_{lex}$ deducidos a partir del orden usual en $\mathbb{N}$. Sea $X = \{(0, n), (1, n-1), \ldots, (n-1, 1), (n, 0)\}$.

1. Calcula el conjunto de cotas inferiores de X en $\mathbb{N} \times \mathbb{N}$ respecto del orden lexicográfico y con respecto al orden producto.
2. Calcula ínfimo y mínimo (caso de existir) de $X \subseteq \mathbb{N} \times \mathbb{N}$, respecto del orden lexicográfico y del orden producto cartesiano.
3. Calcula los elementos maximales y minimales de X respecto a esos dos órdenes.

2. Retículos

Definición 1. Un retículo es un conjunto ordenado, $(L, \leq)$ en el que cualquier conjunto finito tiene supremo e ínfimo.

Si $(L, \leq)$ es un retículo y $x, y \in L$, denotaremos por $x \vee y$ al supremo del conjunto $\{x, y\}$ y por $x \wedge y$ al ínfimo del conjunto $\{x, y\}$.

Nótese que $x \vee y$ está definido por la propiedad:

$$x \leq x \vee y;\ y \leq x \vee y \qquad (x \leq z \text{ e } y \leq z) \Longrightarrow x \vee y \leq z$$

La primera parte dice que $x \vee y$ es una cota superior del conjunto $\{x, y\}$, mientras que la segunda dice que es la menor de las cotas superiores.

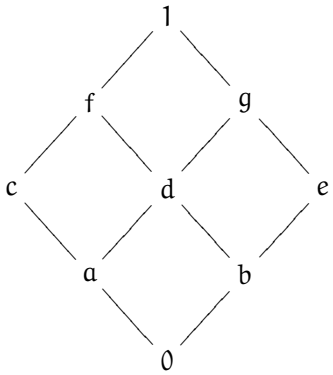
2.1. Propiedades de retículos.

Si $(L, \leq)$ es un retículo, las operaciones $\vee$ y $\wedge$ satisfacen las siguienes propiedades:

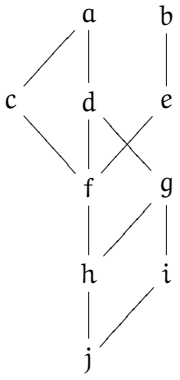
$$\begin{array}{rl}
\text{Conmutativa} & \begin{cases} x \vee y = y \vee x \\ x \wedge y = y \wedge x \end{cases} \\
\text{Asociativa} & \begin{cases} x \vee (y \vee z) = (x \vee y) \vee z \\ x \wedge (y \wedge z) = (x \wedge y) \wedge z \end{cases} \\
\text{Absorción} & \begin{cases} x \vee (x \wedge y) = x \\ x \wedge (x \vee y) = x \end{cases} \\
\text{Idempotencia} & \begin{cases} x \vee x = x \\ x \wedge x = x \end{cases}
\end{array}$$

Ejercicio 28:

1. Prueba que si X es un conjunto totalmente ordenado, entonces para cada $x, y \in X$, $x \vee y = \text{máx}(\{x, y\})$ mientras que $x \wedge y = \text{mín}(\{x, y\})$. Demuestra que X es un retículo.
2. El conjunto ordenado $(\mathbb{N}, |)$ es un retículo. Prueba que en este caso se tiene que $x \vee y = \text{mcm}(x, y)$ mientras que $x \wedge y = \text{mcD}(x, y)$. De la misma forma, si $n \in \mathbb{N}$ entonces $D(n)$, con el orden dado por la divisibilidad es un retículo.
3. Para X es un conjunto, demuestra $\mathcal{P}(X)$ es un retículo. Prueba primero que $A \vee B = A \cup B$ y $A \wedge B = A \cap B$, para cualesquiera A y B subconjuntos de X.
4. Prueba que el conjunto ordenado cuyo diagrama de Hasse es



   es un retículo.
5. Demuestra que conjunto ordenado cuyo diagrama de Hasse es



   no es un retículo.

Nótese que si $(L, \leq)$ es un retículo, entonces dados $x, y \in L$ se verifica que $x \leq y$ si, y sólo si, $x \vee y = y$, o si queremos, $x \leq y$ si, y sólo si, $x \wedge y = x$. Es decir, podemos recuperar el orden dentro del retículo a partir del conocimiento de las operaciones supremo o ínfimo.

La siguiente proposición nos da condiciones suficientes para que dos operaciones definidas en un conjunto puedan ser el supremo y el ínfimo de alguna relación de orden en ese conjunto.

Proposicion. Sea L un conjunto en el que tenemos definidas dos operaciones $\vee$ y $\wedge$ que satisfacen las propiedades conmutativa, asociativa, idempotencia y de absorción. Supongamos que en L definimos la relación

$$x \leq y \quad \text{si } x \vee y = y$$

Entonces, $(L, \leq)$ es un retículo donde las operaciones supremo e ínfimo vienen dadas por $\vee$ y $\wedge$ respectivamente.

Nótese que se tiene que $x \vee y = y$ si, y sólo si, $x \wedge y = x$, luego podría haberse hecho la demostración definiendo la relación

$$x \leq y \quad \text{si } x \wedge y = x$$

Nótese también que la propiedad de idempotencia se puede deducir a partir de la de absorción, pues

$$x \vee x = x \vee [x \wedge (x \vee x)] = x$$

luego podemos demostrar la proposición anterior partiendo de que las operaciones $\vee$ y $\wedge$ satisfacen las propiedades asociativa, conmutativa y de absorción.

Esta proposición permite definir un retículo, bien dando la relación de orden, bien dando las operaciones $\vee$ y $\wedge$.

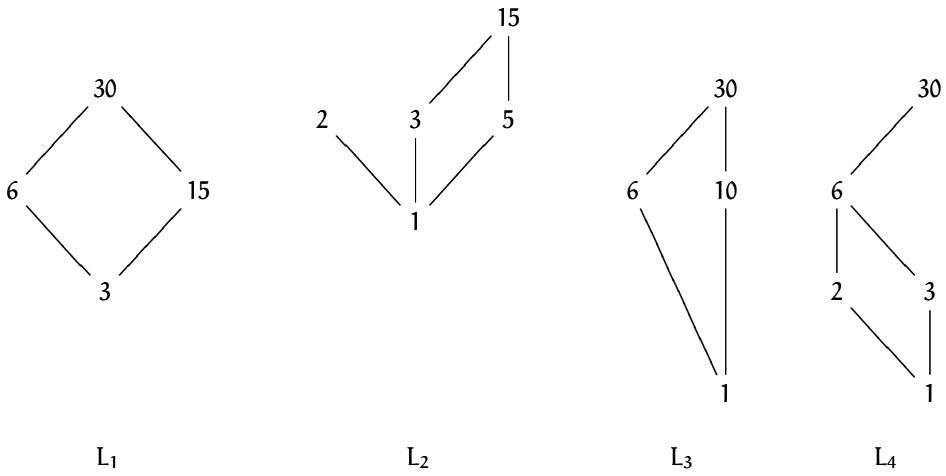
Si $(L, \leq)$ es un retículo y L tiene máximo, denotaremos a éste por 1, mientras que si tiene mínimo lo denotaremos por 0. Se tiene entonces, $x \vee 1 = 1$, $x \wedge 1 = x$, $x \vee 0 = x$ y $x \wedge 0 = 0$.

Un retículo finito siempre tiene máximo y mínimo. Si el retículo es infinito, puede tenerlo o no. Así, por ejemplo, $(\mathbb{N}, \leq)$ tiene mínimo pero no tiene máximo; $(\mathbb{Z}, \leq)$ no tiene ni mínimo ni máximo. El retículo $(\mathbb{N}, |)$ es infinito y tiene máximo y mínimo. En este caso, el máximo es 0 mientras que el mínimo es 1.

Subretículo. Sea $(L, \leq)$ un retículo, y $L' \subseteq L$ un subconjunto de L. Entonces L' es un subrretículo si para cualesquiera $x, y \in L'$ se verifica que $x \vee y \in L'$ y $x \wedge y \in L'$.

`maxima 33:` Consideramos el retículo D(30).

Sean $L_1 = \{3, 6, 15, 30\}$, $L_2 = \{1, 2, 3, 5, 15\}$, $L_3 = \{1, 6, 10, 30\}$ y $L_4 = \{1, 2, 3, 6, 30\}$. Sus diagramas de Hasse son:



L_1 L_2 L_3 L_4

Entonces L_1 y L_4 son subretículos de $D(30)$, mientras que L_2 y L_3 no lo son.

```
(%i29) condsubreticulosup(rel,con,amb):=subset(cartesian_product(con,con),
       lambda([x],not(elementp(supremo(rel,{x[1],x[2]},amb),con))))$
(%i30) condsubreticuloinf(rel,con,amb):=subset(cartesian_product(con,con),
       lambda([x],not(elementp(infimo(rel,{x[1],x[2]},amb),con))))$
(%i31) subreticulop(rel,con,amb):=emptyp(condsubreticulosup(rel,con,amb)) and
       emptyp(condsubreticuloinf(rel,con,amb))$
(%i32) subreticulop(div,{3,6,15,30},divisors(30));
(%o32) true

(%i33) condsubreticulo(div,{1,2,3,5,15},divisors(30));
(%o33) condsubreticulo(div, 1, 2, 3, 5, 15, 1, 2, 3, 5, 6, 10, 15, 30)

(%i34) supremo(div,{2,3},divisors(30));
(%o34) 6

(%i35) subreticulop(div,{1,6,10,30},divisors(30));
(%o35) false

(%i36) condsubreticuloinf(div,{1,6,10,30},divisors(30));
(%o36) {[6, 10], [10, 6]}

(%i37) subreticulop(div,{1,2,3,6,30},divisors(30));
(%o37) true
```

Retículo distributivo. Sea L un retículo. Se dice que L es distributivo si para cualesquiera $x, y, z \in L$ se verifica que

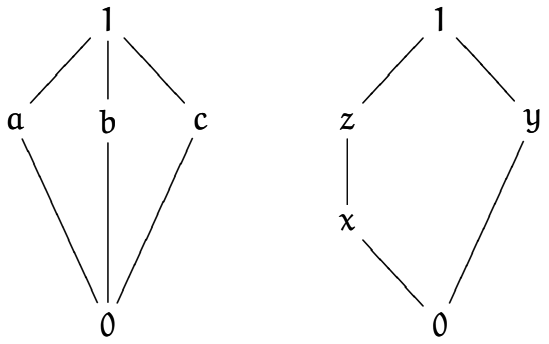
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad \text{y} \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

Basta con que se de una de las dos posibles propiedades distributivas para que se de la otra.

Ejercicio 29:

1. Prueba que si L es un conjunto totalmente ordenado, entonces L es un retículo distributivo.
2. Demuestra que el retículo $(\mathbb{N}, |)$ es un retículo distributivo.
   De igual forma, para cada número natural $n \in \mathbb{N}$, el retículo $D(n)$ es distributivo.
3. Prueba que si X es un conjunto, entonces $(\mathcal{P}(X), \subseteq)$ es un retículo distributivo.

Consideramos los siguientes retículos:



denominados respectivamente *diamante* y *pentágono*. En el ejemplo anterior hemos visto que el diamante no es distributivo. En cuanto al pentágono, se tiene que

$$x \vee (y \wedge z) = x \vee 0 = x \qquad (x \vee y) \wedge (x \vee z) = 1 \wedge z = z$$

luego tampoco es distributivo.

En general, se tiene que un retículo es distributivo si no contiene como subretículos ni al pentágono ni al diamante. En el apartado anterior hemos visto como el retículo de subespacios vectoriales de un espacio vectorial tiene al diamante como subretículo.

2.2. Propiedad cancelativa. Sea L un retículo distributivo, y sen $x, y, z \in L$ tales que $x \vee y = x \vee z$ y $x \wedge y = x \wedge z$. Entonces $y = z$.

En el diamante se tiene que $a \vee b = a \vee c = 1$, y $a \wedge b = a \wedge c = 0$, y sin embargo, $b \neq c$.
En el pentágono, $y \vee x = y \vee z = 1$ e $y \wedge x = y \wedge z = 0$, y sin embargo, $x \neq z$.

Retículo complementado. Sea L un retículo que tiene máximo y mínimo (a los que denotaremos por 1 y 0 respectivamente), y $x \in L$. Se dice que $y \in L$ es un complemento de x si $x \vee y = 1$ y $x \wedge y = 0$.

Un reticulo en el que todo elemento tiene complemento se dice complementado.

Obviamente, si y es un complemento de x entonces x es un complemento de y.

Por otra parte, si L es un retículo distributivo y x un elemento de L que tiene complemento, entonces el complemento es único (ver propiedad 2.2).

Si L es un retículo distributivo, y x es un elemento que tiene complemento, denotaremos por x' o $\overline{x}$ al único complemento de x.

Ejercicio 30:

1. Si L tiene máximo (1) y mínimo (0), entonces 0 es un complemento de 1.
2. El retículo $(\mathcal{P}(X), \subseteq)$ es un retículo complementado. Dado $A \in \mathcal{P}(X)$ se verifica que $A \cup (X \setminus A) = X$ y $A \cap (X \setminus A) = \emptyset$. Por ser un retículo distributivo, el commplemento de cada elemento es único.
3. El pentágono y el diamente son retículos complementados. Vemos sin embargo, que los complementos de algunos elementos no son únicos.
   Así, en el diamante, tanto b como c son complementos de a; tanto a como c son complementos de b y tanto a como b son complementos de c.

En el pentágono, tanto x como z son complementos de y. Sin embargo, x y z tienen un único complemento, que es y.

4. Si L es un conjunto totalmente ordenado con más de dos elementos, entonces es un retículo distributivo, pero no es complementado.

maxima 34:

Dado un número natural D(n), el retículo D(n) no tiene por qué ser un retículo complementado. Por ejemplo, D(4) no es complementado (es un conjunto totalmente ordenado con 3 elementos), mientras que D(6) sí lo es.

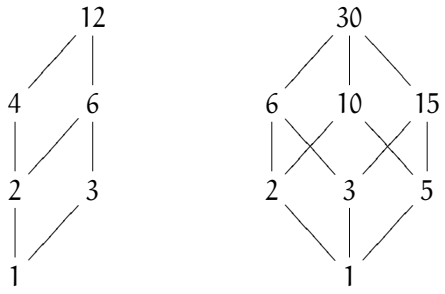
```
(%i38) complementos(x,rel,con):=block(local(max,min),
       max:maximo(rel,con),
       min:minimo(rel,con),
       subset(con,lambda([y],is(supremo(rel,{x,y},con)=max)
       and is(infimo(rel,{x,y},con)=min))))$
(%i39) complementos(2,div,divisors(6));
(%o39) {3}

(%i40) complementos(2,div,divisors(4));
(%o40) {}

(%i41) complementadop(rel,con):=emptyp(subset(con,lambda([x],
       emptyp(complementos(x,rel,con)))))$
(%i42) complementadop(div,divisors(6));
(%o42) true

(%i43) complementadop(div,divisors(4));
(%o43) false
```

En D(12) tienen complemento 1, 3, 4, 12 mientras que no tienen 2, 6. En D(30) todos los elementos tienen complemento.



D(12) D(30)

```
(%i44) complementadop(div,divisors(12));
(%o44) false

(%i45) notienencomplemento(rel,con):=subset(con,lambda([x],
       emptyp(complementos(x,rel,con))))$
(%i46) notienencomplemento(div,divisors(12));
(%o46) {2, 6}
```

```
(%i47) complementadop(div,divisors(30));
(%o47) true
```

Ejercicio 31: Se pide, determinar qué elementos de $D(n)$ tienen complemento, y a partir de ahí, determinar para qué valores de n es $D(n)$ un retículo complementado.

2.3. Producto de conjuntos ordenados. Sea $(L_1, \leq)$ y $(L_2, \leq)$ dos conjuntos ordenados. Consideramos en $L_1 \times L_2$ el orden producto. Entonces:

- Si L_1 y L_2 son retículos, también lo es $L_1 \times L_2$. Las operaciones supremo e ínfimo en $L_1 \times L_2$ vienen dadas por
$$(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2) \qquad (x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2)$$
- Si L_1 y L_2 son retículos distributivos, también lo es $L_1 \times L_2$.
- Si L_1 y L_2 son retículos complementados, también lo es $L_1 \times L_2$.

3. Álgebras de Boole

Definición de álgebra de Boole. Un *álgebra de Boole* es un retículo distributivo y complementado.

Ejercicio 32:

1. Dado un conjunto X, el conjunto $\mathcal{P}(X)$, con el orden dado por la inclusión es un álgebra de Boole.
2. $D(6)$, o $D(30)$ son álgebras de Boole. No es álgebra de Boole $D(4)$ o $D(12)$.

Al igual que los retículos se pueden definir sin mencionar el orden, sino únicamente las operaciones supremo e ínfimo, con las respectivas propiedades, un álgebra de Boole puede definirse también a partir de las operaciones $\vee$ y $\wedge$.

Segunda definición de álgebra de Boole. Sea B un conjunto. Supongamos que en B tenemos definidas dos operaciones, $\vee$ y $\wedge$ tales que:

1. $x \vee (y \vee z) = (x \vee y) \vee z \qquad x \wedge (y \wedge z) = (x \wedge y) \wedge z$
2. $x \vee y = y \vee x \qquad x \wedge y = y \wedge z$
3. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \qquad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
4. $x \vee (x \wedge y) = x \qquad x \wedge (x \vee y) = x$
5. Existen $0, 1 \in B$ tales que $x \vee 0 = x \quad x \wedge 0 = 0 \quad x \vee 1 = 1 \quad x \wedge 1 = x$
6. Para cada $x \in B$ existe $x' \in B$ tal que $x \vee x' = 1$ y $x \wedge x' = 0$.

Es fácil comprobar que las dos definiciones son equivalentes.

Leyes de De Morgan. Sea B un álgebra de Boole, y $x, y \in B$. Entonces:
$$(x \vee y)' = x' \wedge y' \qquad (x \wedge y)' = x' \vee y'$$

Ejercicio 33: Consideremos el conjunto $\mathbb{Z}_2$. En él, consideramos las operaciones
$$x \wedge y = xy \qquad x \vee y = x + y + xy$$
Entonces $\mathbb{Z}_2$, con estas operaciones es un álgebra de Boole. De hecho, es el álgebra de Boole más simple (a excepción de un álgebra de Boole con un elemento). Representaremos a este álgebra de Boole como $\mathbb{B}$.

Nótese que este álgebra de Boole se corresponde con el orden $0 \leq 1$.

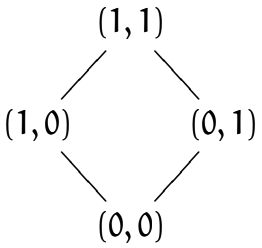
Puesto que el producto de álgebras de Boole es un álgebra de Boole, tenemos, para cada número natural n el álgebra de Boole $\mathbb{B}^n$ que tiene 2^n elementos. En este caso, las operaciones del álgebra de Boole vienen dadas por:

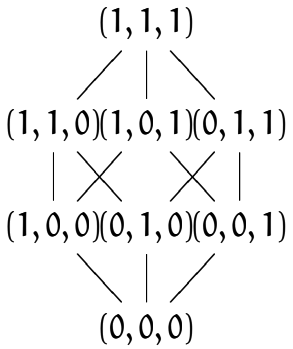
$$(x_1, x_2, \ldots, x_n) \vee (y_1, y_2, \ldots, y_n) = (x_1 \vee y_1, x_2 \vee y_2, \ldots, x_n \vee y_n)$$

$$(x_1, x_2, \ldots, x_n) \wedge (y_1, y_2, \ldots, y_n) = (x_1 \wedge y_1, x_2 \wedge y_2, \ldots, x_n \wedge y_n)$$

$$(x_1, x_2, \ldots x_n)' = (x_1', x_2', \ldots, x_n')$$

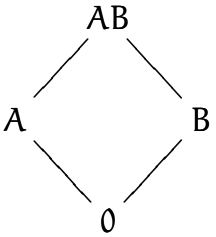
Veamos los diagramas de Hasse de $\mathbb{B}^2$ y $\mathbb{B}^3$.



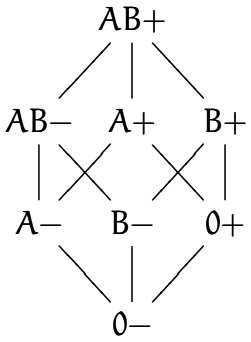


Podemos comparar las estructuras de álgebra de Boole de $\mathbb{B}^2$ y $\mathbb{B}^3$ con las de $\mathcal{P}(\{a, b\})$ y $\mathcal{P}(\{a, b, c\})$.

Consideramos las álgebras de Boole siguientes:



que como podemos ver tienen una estructura semejante a $\mathbb{B}^2$ y $\mathbb{B}$ respectivamente. Su producto, tendrá entonces la misma estructura que $\mathbb{B}^3$. El diagrama de Hasse de dicho álgebra sería



y vemos que los elementos que la forman son los ocho grupos sanguíneos. En este caso, ser *menor o igual* significa *puede donar*. Así, el grupo $0-$ es el donante universal, mientras que el grupo $AB+$ es el receptor universal.

Átomos. Sea B un álgebra de Boole, y $x \in B$. Se dice que x es un átomo si x es un elemento minimal de $B \setminus \{0\}$.

Ejercicio 34: Si X es un conjunto, los átomos del álgebra de Boole $\mathcal{P}(X)$ son los subconjuntos unitarios.

Los átomos del álgebra de Boole $\mathbb{B}^n$ son aquellos que tienen todas las coordenadas nulas salvo una.

maxima 35: En el álgebra de Boole $D(30)$ los átomos son los divisores primos de 30.

```
(%i48) minimales(div,setdifference(divisors(30),{1}));
(%o48) {2,3,5}
```

3.1. Todo elemento es supremo de átomos. Sea B un álgebra de Boole finita, y $x \in B \setminus \{0\}$. Entonces, x se expresa de forma única como supremo de átomos.

Dado cualquier elemento $x \in B \setminus \{0\}$, denotaremos por $\mathcal{A}_x$ al conjunto de todos los átomos de B que son menores o iguales que x.

Este teorema nos dice que si B es un álgebra de Boole finita, y $X = \{a_1, \ldots, a_n\}$ son sus átomos (es decir, $X = \mathcal{A}_1$) entonces los elementos de B son:

$$B = \left\{ \bigvee_{x \in A} x : \ A \in \mathcal{P}(X) \right\}$$

donde se ha empleado la notación $0 = \bigvee_{x \in \emptyset} x$.

Vemos entonces que B tiene tantos elementos como $\mathcal{P}(X)$.

Por tanto, el número de elementos de B es 2^n, donde n es el número de átomos.

Es más, tenemos que las álgebras de Boole B, $\mathbb{B}^n$ y $\mathcal{P}(X)$ con $X = \{1, 2, \ldots, n\}$ son isomorfas.

maxima 36:

```
(%i50) menores(15,div,setdifference(divisors(30),{1}));
(%o50) {3,5,15}

(%i51) supremo(div,{3,5},divisors(30));
(%o51) 15
```

Capítulo 5

Grupo simétrico

Contenidos de este capítulo

1. Grupos

Un grupo es un conjunto no vacío G junto con una operación binaria interna

$$* : G \times G \to G, \quad (g_1, g_2) \mapsto g_1 * g_2,$$

verificando las siguientes propiedades

1. la operación $*$ es asociativa (o equivalentemente, $(G, *)$ es in semigrupo), a saber, $a*(b*c) = (a*b)*c$, para cualesquiera $a, b, c \in G$; esto nos permite transformar $*$ en una operación n-aria, pues para calcular $a_1 * \cdots * a_n$ no tenemos que preocuparnos por poner paréntesis,
2. existe un elemento llamado elemento neutro o identidad, e, verificando que $e*g = g*e = g$ para todo $g \in G$ ($(G, *)$ es un monoide; se puede demostrar que si existe un elemento neutro, sólo existe uno),
3. para todo elemento $g \in G$, existe $g^{-1} \in G$ tal que $g * g^{-1} = e = g^{-1} * g$ (se puede probar que este elemento es único).

A veces nos referiremos a G como $(G, *)$ para indicar con qué operación estamos considerando que es un grupo.

Normalmente a la operación $*$ la denotaremos simplemente por yuxtaposición, y a veces escribiremos 1 para denotar al elemento neutro.

Ejercicio 35: Dados $g_1, g_2 \in G$, demuestra que $(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$.

Si además $*$ es conmutativa, o sea, $g_1 * g_2 = g_2 * g_1$ para cualesquiera $g_1, g_2 \in G$, entonces decimos que G es un grupo abeliano o conmutativo. En este caso usaremos 0 para denotar la identidad, y $+$ en lugar de $*$.

Ejemplos de grupos abelianos son $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$ para todo $n \in \mathbb{N}$. No son grupos ni $(\mathbb{N}, +)$ ni $(\mathbb{Z}, \cdot)$ (¿por qué?).

Al producto cartesiano de dos grupos se le puede dotar de estructura de grupo.

Ejercicio 36: Si $(G_1, *_1)$ y $(G_2, *_2)$ son grupos, demuestra que $(G_1 \times G_2, *)$, con $*$ definida como $(a, b) * (c, d) = (a *_1 b, c *_2 d)$, es también un grupo.

2. Subgrupos

Un subconjunto H de un grupo G es un subgrupo si para cualesquiera $h_1, h_2 \in H$, $h_1 h_2^{-1} \in H$. Esto equivale a decir que $1 \in H$, H es cerrado para la operación que hace de G un grupo, y también es cerrado para cálculo de inversos. De esta forma H es un grupo con la misma operación de G.

Ejercicio 37: El conjunto de los números enteros es un subgrupo de $\mathbb{Q}$ con la suma. Sin embargo, $\mathbb{Z}$ no es un subgrupo de $\mathbb{Q}$ con el producto.

Teorema de Lagrange. Si H es un subgrupo de G, entonces $\#H$ divide a $\#G$.

Dado un subconjunto X de un grupo G, se define el subgrupo generado por X, que denotamos por $\langle X \rangle$, al menor subgrupo de G que contiene a X. Como la intersección de subgrupos vuelve a ser un subgrupo, se tiene que $\langle X \rangle$ es la intersección de todos los subgrupos de G que contienen a X.

Ejercicio 38: Demuestra que $\langle X \rangle = \{x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} \mid n \in \mathbb{N}, x_1, \ldots, x_n \in X, \epsilon_1, \ldots, \epsilon_n \in \{1, -1\}\}$ (para $n = 0$, el producto de n elemento se entiende como 1).

Si H es un subgrupo de G y $X \subseteq G$ es tal que $H = \langle X \rangle$, entonces decimos que X es un sistema de generadores de H. Si $X = \{x_1, \ldots, x_n\}$ para algún entero n positivo, entonces escribiremos $\langle x_1, \ldots, x_n \rangle$ en vez de $\langle X \rangle$. Además, decimos que H es cíclico si admite un sistema de generadores de la forma $X = \{x\}$.

Ejercicio 39: Demuestra que $(\mathbb{Z}, +)$ es un grupo cíclico, y que todo subgrupo suyo es cíclico (pista: usa la identidad de Bézout para probar que está generado por el máximo común divisor de sus elementos).

Ejercicio 40: Demuestra que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (suma componente a componente) no es un grupo cíclico, mientras que $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ sí que lo es.

Orden de un elemento. Dado un grupo G y un elemento $g \in G$, se define el orden de g en G como el menor entero positivo n tal que $g^n = 1$ (g^n es el producto de g consigo mismo n veces). En caso de que no exista ese entero positivo, decimos que g tiene orden infinito.

Ejercicio 41: Demuestra que el orden de g en G coincide con $\#\langle g \rangle$.

maxima 37: Calculemos el orden de todos los elementos de $\mathbb{Z}_{10}$. Sabemos por el Teorema de Lagrange, y por el ejercicio anterior, que el orden de esos elementos divide a 10, el cardinal de $\mathbb{Z}_{10}$. Luego como mucho vale 10.

Empecemos por ejemplo con el 2.

```
(%i1)  setify(makelist(mod(2*i,10),i,0,9));
(%o1)  {0,2,4,6,8}

(%i2)  length(%);
(%o2)  5
```

Que tiene orden 5. Podemos automatizar el proceso y escribir una lista con cada elemento y su orden.

```
(%i3)  makelist([j,length(setify(makelist(mod(j*i,10),i,0,9)))],j,0,9);
(%o3)  [[0, 1], [1, 10], [2, 5], [3, 10], [4, 5], [5, 2], [6, 5], [7, 10], [8, 5], [9, 10]]
```

Así que los posibles órdenes son 1, 2, 5 y 10 (todos los posibles divisores de 10).

Ejercicio 42: ¿Cuál es en general el orden de m en $\mathbb{Z}_n$?

3. El grupo simétrico

Sea X un conjunto no vacío. Definimos S_X como el conjunto de todas las aplicaciones biyectivas de X en X. Este conjunto, junto con la operación composición de aplicaciones, es un grupo.

A los elementos de S_X se les conoce como permutaciones del conjunto X. El conjunto S_X es el grupo simétrico o de permutaciones en X.

En el caso en que $X = \{1, \ldots, n\}$, escribimos S_n en vez de S_X, y lo llamaremos grupo simétrico de orden n.

A las permutaciones $\sigma \in S_n$ las vamos representar de una forma especial como una matriz con dos filas en la que en la primera fila aparecen los enteros del 1 al n, y en la segunda fila, en la columna i-ésima el elemento $\sigma(i)$.

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & n \end{pmatrix}.$$

Para calcular el inverso de σ representado de esta forma, simplemente tenemos que intercambiar la primera con la segunda fila, y después reordenar las columnas de forma que en la primera fila aparezcan ordenadamente los enteros del 1 al n.

Para multiplicar dos permutaciones se sigue el orden de derecha a izquierda que van tomando las imágenes de cada uno de los elementos del conjunto X (ojo que en algunos libros es al revés, gappor ejemplo usa el orden inverso al que usamos nosotros).

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

ya que el 1 va al 3 por la primera (empezando por la derecha) y la segunda deja el 3 invariante, el 2 se queda invariante por la primera, y la segunda lo envía al 1, y por último el 3 va al 1 por la primera, mientras que la segunda lo manda al 2.

El soporte de una permutación es el conjunto de los $x \in X$ tales que $\sigma(x) \neq x$. Dos permutaciones se dicen disjuntas, si sus soportes lo son.

Ciclos. Un ciclo es una permutación $\sigma \in S_n$ de forma que existe $Y = \{i_1, \ldots, i_k\}$ con $\#Y = k$ (no se repiten elementos en esa lista) tal que $\sigma(i_j) = i_{j+1}$ para todo $j \in \{1, \ldots, k-1\}$, $\sigma(i_k) = i_1$, y $\sigma(x) = x$ para todo $x \in X \setminus Y$. Esto es, σ mueve cíclicamente los elementos de Y y deja inalterado el resto de elementos de X. Diremos que σ es un ciclo de longitud k, y lo denotaremos por $\sigma = (i_1, \ldots, i_k)$.

El inverso del ciclo $(i_1, i_2, \ldots, i_k)$ es $(i_k, i_{k-1}, \ldots, i_1)$. Además, $\tau^k = 1$ (la identidad).

Nótese además que $(i_i, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \cdots$.

Ejercicio 43: Si tenemos dos ciclos disjuntos σ y δ, entonces, $\sigma\delta = \delta\sigma$.

Producto de ciclos disjuntos. Toda permutación se puede expresar de forma única (salvo el orden de los factores) como producto de ciclos disjuntos.

Ejercicio 44: Si σ se pone como producto de $\sigma_1, \ldots, \sigma_c$ ciclos disjuntos, con σ_i de longitud l_i, entonces el orden de σ es el mínimo común múltiplo de $\{l_1, \ldots, l_c\}$.

Una transposición es un es un ciclo de longitud 2. Nótese que si $\tau = (a, b)$ es una transposición, entonces $\tau^{-1} = \tau = (a, b)$.

Todo ciclo $(i_1, i_2, \ldots, i_k)$ se puede expresar como producto de transposiciones, por ejemplo,

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2).$$

Así toda permutación es producto de transposiciones. Si bien el número de éstas puede variar, por ser por ejemplo, $1 = (1,2)(1,2)$, la paridad del número de éstas es invariante. Definimos así la signatura de una permutación σ como $(-1)^t$, con t el número de transposiciones en un descomposición de σ como producto de transposiciones.

gap 1: En gap, las permutaciones se pueden escribir de muchas formas. O bien como producto de ciclos disjuntos, o usando funciones específicas para crear permutaciones.

```
gap> MappingPermListList([1,2,3,4],[2,3,1,4]);
(1,2,3)
gap> PermList([2,3,1,4]);
(1,2,3)
gap> (1,2,3)(4,6);
(1,2,3)(4,6)
gap> ListPerm((1,2,3)(4,6));
[ 2, 3, 1, 6, 5, 4 ]
gap> PermList(last);
(1,2,3)(4,6)
```

El operador '*' se usa para la composición (hay que tener cuidado en el orden en que se compone). En el ejemplo anterior, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$,

```
gap> PermList([3,2,1])*PermList([2,1,3]);
(1,3,2)
gap> ListPerm(last);
[ 3, 1, 2 ]
```

El operador '^' se puede usar para calcular la imagen de un elemento por una permutación.

```
gap> p:=(1,2,3)*(3,4);
(1,2,4,3)
gap> 3^p;
1
```

El orden de una permutación (orden como elemento dentro de S_n) y su signatura se pueden calcular de la siguiente forma.

```
gap> SignPerm((1,2,3)(4,6));
-1
gap> Order((1,2,3)(4,6));
6
gap> G:=SymmetricGroup(4);
Sym( [ 1 .. 4 ] )
```


```
gap> Elements(G);
[ (), (3,4), (2,3), (2,3,4), (2,4,3), (2,4), (1,2), (1,2)(3,4), (1,2,3),
  (1,2,3,4), (1,2,4,3), (1,2,4), (1,3,2), (1,3,4,2), (1,3), (1,3,4),
  (1,3)(2,4), (1,3,2,4), (1,4,3,2), (1,4,2), (1,4,3), (1,4), (1,4,2,3),
  (1,4)(2,3) ]
gap> Filtered(G,x->Order(x)=4);
[ (1,2,3,4), (1,2,4,3), (1,3,4,2), (1,3,2,4), (1,4,3,2), (1,4,2,3) ]
```

Podemos definir un grupo generado por varias permutaciones, calcular su orden, o comprobar si es abeliano (y muchas otras propiedades).

```
gap> g:=Group((1,2,3),(4,5));
Group([ (1,2,3), (4,5) ])
gap> Order(g);
6
gap> Elements(g);
[ (), (4,5), (1,2,3), (1,2,3)(4,5), (1,3,2), (1,3,2)(4,5) ]
gap> IsAbelian(g);
true
```

Con la orden `IsCyclic` podemos saber si un grupo es cíclico.

```
gap> g:=Group((1,2,3),(4,5));;
gap> IsCyclic(g);
true
gap> DirectProduct(CyclicGroup(2),CyclicGroup(2));
<pc group of size 4 with 2 generators>
gap> IsCyclic(last);
false
```

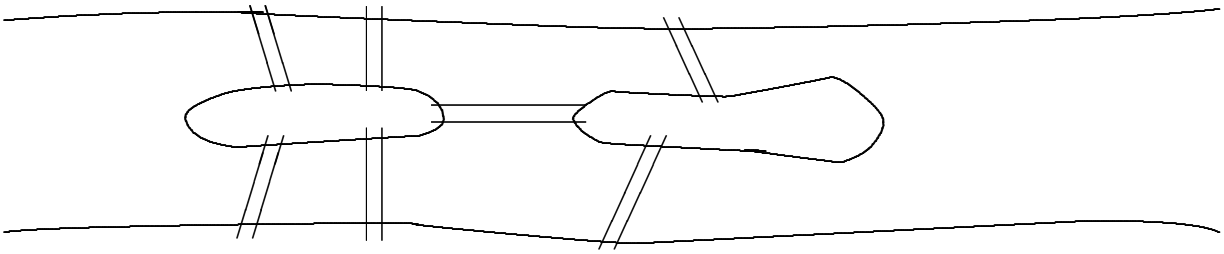
Capítulo 6

Teoría de Grafos

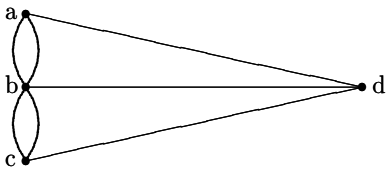
Contenidos de este capítulo

El inicio de la Teoría de Grafos tuvo lugar en 1736, en un artículo de Leonhard Euler. El trabajo surgió de un problema conocido como el *problema de los puentes de Königsberg.*

> Durante el Siglo XVIII, la ciudad de Königsberg, en Prusia Oriental estaba dividida en cuatro zonas por el río Pregel. Había siete puentes que comunicaban estas regiones, tal y como se muestra en el dibujo. Los habitantes de la ciudad hacían paseos dominicales tratando de encontrar una forma de caminar por la ciudad, cruzando cada puente una sola vez, y regresando al lugar de partida.



Para resolver este problema, Euler representó las cuatro zonas como cuatro puntos, y los puentes como aristas que unen los puntos, tal y como se muestra en la figura.



Más adelante veremos cómo resolver el problema.

1. Generalidades sobre grafos

Volvamos a la representación que hizo Euler. En ella intervienen cuatro puntos (a los que denominaremos vértices), a saber, $\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}$ y siete aristas o lados que conectan algunos de los vértices. Esto da pie a la siguiente definición de grafo.

1.1. Definición de grafo. Un grafo G es un par (V, E), donde V y E son conjuntos, junto con una aplicación

$$\gamma_G : E \to \{\{u, v\} : u, v \in V\}.$$

Al conjunto V se le llama conjunto de vértices; al conjunto E conjunto de lados o aristas, y a la aplicación γ_G (o simplemente γ) aplicación de incidencia.

En el caso de los puentes de Königsberg, el grafo correspondiente tiene como conjunto de vértices al conjunto $V = \{a, b, c, d\}$, como conjunto de lados el conjunto $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ y la aplicación de incidencia es la dada por:

$$\gamma_G(e_1) = \gamma_G(e_2) = \{a, b\} \quad \gamma_G(e_3) = \gamma_G(e_4) = \{b, c\} \quad \gamma_G(e_5) = \{a, d\} \quad \gamma_G(e_6) = \{b, d\} \quad \gamma_G(e_7) = \{c, d\}.$$

Si e_1 y e_2 son dos lados tales que $\gamma_G(e_1) = \gamma_G(e_2)$, se dice que son *lados paralelos*.

Un lado tal que $\gamma_G(e) = \{v\}$ se dice *un lazo*.

Algunos autores, al definir un grafo, no incluyen la posibilidad de que tenga lados paralelos ni lazos. En tal caso, lo que aquí hemos definido como un grafo lo denominan como *multigrafo*.

maxima 38: Vamos a pintar un grafo que tenga por vértices los elementos de $\mathcal{P}(\{1, 2, 3\}$, y un lado conecta A y B si $A \subseteq B$ (o $B \subseteq A$, al no ser un grafo dirigido).

Para definir un grafo necesitamos dos listas, una con los vértices y otra con los lados.

```
(%i1)  v:powerset({1,2,3});
```
(%o1) $\{\{\}, \{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 3\}, \{2\}, \{2, 3\}, \{3\}\}$

```
(%i2)  vl:listify(v)$
(%i3)  s8:setify(makelist(i,i,1,8))$
(%i4)  vertices:makelist([i,vl[i]],i,1,8);
```
(%o4) $[[1, \{\}], [2, \{1\}], [3, \{1, 2\}], [4, \{1, 2, 3\}], [5, \{1, 3\}], [6, \{2\}], [7, \{2, 3\}], [8, \{3\}]]$

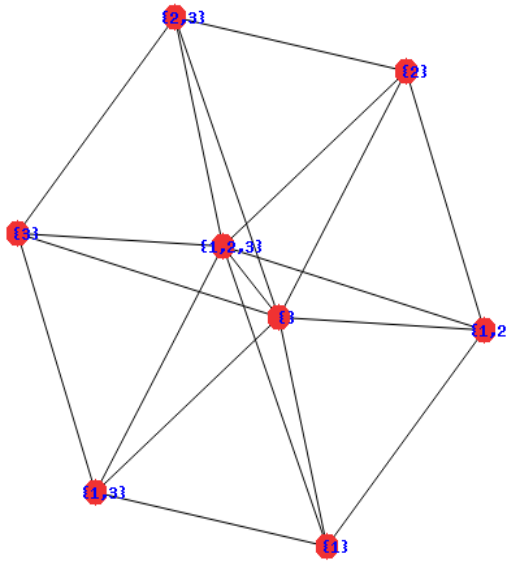
Ya tenemos los vértices del 1 al 8 etiquetados con cada uno de los elementos de $\mathcal{P}(\{1, 2, 3\})$. Ahora vamos a construir los lados. Para ello extraemos del producto cartesiano de $\mathcal{P}(\{1, 2, 3\})$ aquellos que son lados de nuestro grafo.

```
(%i5)  l:subset(cartesian_product(s8,s8),
       lambda([x],subsetp(vl[x[1]],vl[x[2]]) and not(is(vl[x[1]]=vl[x[2]]))));
```
(%o5) $\{[1, 2], [1, 3], [1, 4], [1, 5], [1, 6], [1, 7], [1, 8], [2, 3], [2, 4], [2, 5],$
$[3, 4], [5, 4], [6, 3], [6, 4], [6, 7], [7, 4], [8, 4], [8, 5], [8, 7]\}$

```
(%i6)  lados:listify(l)$
(%i7)  load(graphs)$
(%i8)  g:create_graph(vertices,lados);
```
(%o8) GRAPH(8 vertices, 19 edges)

Por último pintamos el grafo.

```
(%i9)  draw_graph(g,show_labels=true);
```



Grafo dirigido. Un grafo dirigido u orientado es un par (V, E), donde V y E son conjuntos, junto con dos aplicaciones $s, t : E \to V$.

Al conjunto V se le llama conjunto de vértices, al conjunto E conjunto de lados, y a las aplicaciones s y t aplicaciones dominio y codominio ("source" y "target").

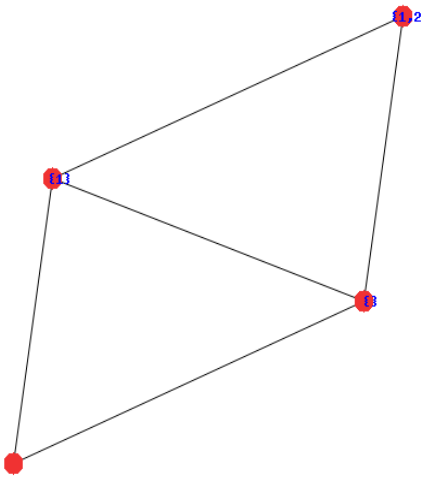
Subgrafo. Sea $G = (V, E)$ un grafo con aplicación de incidencia γ_G. Un subgrafo de G es un nuevo grafo $G' = (V', E')$ donde $V' \subseteq V$, $E' \subseteq E$ y se verifica que $\gamma_{G'}(e) = \gamma_G(e)$ para cualquier $e \in E'$.

Si $G' = (V', E')$ es un subgrafo de un grafo $G = (V, E)$, se dice que es un subgrafo completo si dado $e \in E$ tal que $\gamma_G(e) \subseteq V'$, se verifica que $e \in E'$. Dicho de otra forma, si tiene todos los lados que tenía G y que unen vértices de V'.

Observación: Un subgrafo completo está completamente determinado por el conjunto de vértices. Así, para determinar un subgrafo de un grafo G en ocasiones explicitaremos únicamente el conjunto de vértices de dicho subgrafo, sobreentendiendo que se trata del subgrafo completo con dicho conjunto de vértices.

maxima 39:

```
(%i20) h:induced_subgraph([1,2,3,5],g);
(%o20) GRAPH(4 vertices, 5 edges)
(%i22) draw_graph(h,show_label=true);
```



(%o22) done

Caminos. Sea G un grafo. Un camino de longitud n es una sucesión de lados $e_1e_2\cdots e_n$, junto con una sucesión de vértices $v_1v_2\cdots v_{n+1}$ tales que $\gamma_G(e_i) = \{v_i, v_{i+1}\}$.

En tal caso se dice que el camino $e_1e_2\cdots e_n$ es un camino del vértice v_1 al vértice v_{n+1}.

Se considera un camino de longitud cero de v a v a aquel cuya sucesión de vértices es v y cuya sucesión de lados es vacía.

Para dar un camino en un grafo, en ocasiones daremos únicamente la sucesión de vértices, y en ocasiones daremos únicamente la sucesión de lados.

Nótese que si $e_1e_2\cdots e_n$ es un camino de u a v, entonces $e_ne_{n-1}\cdots e_2e_1$ es un camino de v a u.

Un camino en el que no aparecen lados repetidos se llama *recorrido*.

Un recorrido en el que no hay vértices repetidos (salvo eventualmente el primero y el último) se llama *camino simple*.

Un camino en el que coinciden el primer y el último vértice se llama *camino cerrado*.

Un recorrido que es a la vez camino cerrado se llama *circuito*.

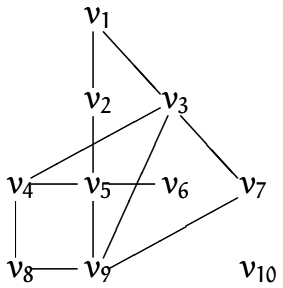
Un circuito que a su vez es camino simple es un *ciclo*.

La siguiente tabla puede ayudar a aclarar estas definiciones.

Vértices repetidos	Aristas repetidas	Abierto	Nombre
			Camino
		No	Camino cerrado
	No		Recorrido
	No	No	Circuito
No	No		Camino simple
No	No	No	Ciclo

Por tanto, en un circuito puede haber o puede no haber vértices repetidos. Sin embargo, no puede haber aristas repetidas. Se tiene entonces, por ejemplo, que todo ciclo es un circuito, es un camino cerrado y es un camino.

Consideramos el siguiente grafo:



La sucesión $v_7v_3v_9v_5v_4v_8v_9v_3$ es un camino de longitud 7 que une v_7 con v_6. No es recorrido, pues el lado que une v_3 con v_9 aparece dos veces en el camino.

La sucesión $v_1v_3v_9v_8v_4v_3v_7$ es un camino de longitud 6 que une v_1 con v_7. Es un recorrido, pues ningún lado se repite. Sin embargo, el camino pasa dos veces por el vértice v_3. No es por tanto un camino simple.

$v_3v_4v_8v_9$ es un camino simple de longitud 3.

La sucesión $v_1v_3v_7v_9v_3v_4v_5v_2v_1$ es un camino cerrado de longitud 8. Es además un circuito, pues ningún lado se encuentra repetido. No es un ciclo, ya que el vértice v_3 se repite.

Un ejemplo de ciclo podría ser $v_1v_2v_5v_9v_7v_3v_1$.

Ejercicio 45: Sea G un grafo. Supongamos que existe un camino de u a v. Entonces existe un camino simple de u a v.

Ejercicio 46: Sea G un grafo, y sean u y v dos vértices distintos. Supongamos que tenemos dos caminos simples distintos de u a v. Entonces existe un ciclo en G.

En el ejemplo anterior teníamos un camino de longitud 6 que une v_1 con v_7 ($v_1v_3v_9v_8v_4v_3v_7$). Este camino no es simple, pues el vértice v_3 está repetido. Eliminamos los vértices que se encuentran entre las dos apariciones de v_3 y obtenemos el camino $v_1v_3v_7$, que es un camino simple que une v_1 con v_7.

Por otra parte, tenemos dos caminos simples que unen v_3 con v_8, como son $v_3v_4v_8$ y $v_3v_9v_8$. A partir de estos dos caminos podemos obtener el ciclo $v_3v_4v_8v_9v_3$, recorriendo en primer lugar uno de los caminos que une v_3 con v_8, y recorriendo a continuación el otro en sentido contrario.

Nótese que si partimos de los caminos simple $v_3v_4v_8$ y $v_3v_1v_2v_5v_4v_8$ y repetimos lo hecho en el párrafo precedente obtenemos el camino cerrado $v_3v_4v_8v_4v_5v_2v_1v_3$ que no es un ciclo, pues el vértice v_4 está repetido (o el lado v_4v_8). Sin embargo, la existencia de los dos caminos simples sí nos da la existencia de un ciclo, a saber, $v_3v_4v_5v_2v_1v_3$.

Grafos conexos. Sea G un grafo. Se dice que G es conexo, si dados u y v dos vértices de G existe al menos un camino de u a v.

En general, si G es un grafo, podemos definir en el conjunto de vértices la relación:

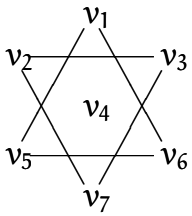
$$uRv \text{ si existe un camino de } u \text{ a } v.$$

Ejercicio 47: Prueba que esta relación es de equivalencia.

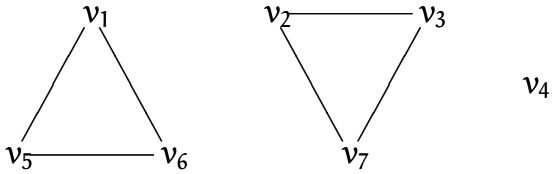
Se tiene entonces que un grafo es conexo si el conjunto cociente por la relación que acabamos de definir tiene un solo elemento.

A partir de esta relación, podemos considerar, para cada clase de equivalencia, el subgrafo (completo) determinado por los vértices de dicha clase de equivalencia. Cada uno de estos grafos es lo que se denomina una *componente conexa de* G.

Por ejemplo, el grafo



tiene tres componentes conexas. Éstas son



maxima 40:

```
(%i1)  load(graphs)$
(%i2)  g:graph_union(complete_graph(4),cycle_graph(4),path_graph(3));
(%o2)  GRAPH(11 vertices, 12 edges)
```

(Ya veremos más adelante la definición de grafo completo.)

```
(%i3)  print_graph(g);
Graph on 11 vertices with 12 edges.
Adjacencies:
7 : 4 6
6 : 7 5
5 : 6 4
4 : 7 5
10 : 9
9 : 10 8
8 : 9
0 : 1 2 3
1 : 0 2 3
2 : 0 1 3
3 : 0 1 2
(%o3)  done
(%i4)  is_connected(g);
(%o4)  false
(%i5)  connected_components(g);
(%o5)  [[1, 2, 3, 0], [8, 9, 10], [4, 5, 6, 7]]
(%i6)  is_connected(induced_subgraph([8,9,10],g));
(%o6)  true
(%i7)  is_connected(induced_subgraph([8,9,10,4],g));
(%o7)  false
```

2. Matrices asociadas a grafos

En esta sección vamos a ver cómo podemos representar los grafos finitos mediante matrices. A partir de estas matrices podremos obtener propiedades sobre los grafos.

Matriz de adyacencia. Sea G un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \cdots, v_n\}$. Se define su *matriz de adyacencia* como la matriz $A \in \mathcal{M}_n(\mathbb{N})$ cuyo coeficiente (i,j) es igual al número de lados e que unen v_i con v_j (es decir, que verifican que $f(e) = \{v_i, v_j\}$).

Observaciones:

1. La matriz de adyacencia de un grafo es una matriz simétrica, pues cada lado que une v_i con v_j une también v_j con v_i.
2. Si tomáramos otra ordenación de los vértices, la matriz de adyacencia es diferente. Por tanto, un grafo puede tener varias matrices de adyacencia. En general, si A y C son dos matrices de adyacencia de un mismo grafo, entonces existe una matriz de permutación P tal que $P^{-1}CP = A$ (una matriz de permutación es una matriz que tiene en cada fila y en cada columna un coeficiente que vale "uno" y el resto toman el valor "cero". Es una matriz que se obtiene a partir de la matriz identidad realizando intercambio de filas y/o columnas).
3. La existencia de lados paralelos se traduce en la matriz de adyacencia en la existencia de coeficientes mayores que 1. De la misma forma, la existencia de lazos se traduce en que algún elemento de la diagonal principal de la matriz de adyacencia es distinto de cero.
4. Si tenemos un grafo dirigido, también podemos definir su matriz de adyacencia. En este caso, el coeficiente a_{ij} es el número de lados que verifican que $s(e) = v_i$ y $t(e) = v_j$. En este caso, la matriz no tiene porqué ser simétrica.
5. La matriz de adyacencia de un grafo determina a éste. Además, toda matriz cuadrada con coeficientes en $\mathbb{N}$ es la matriz de adyacencia de un grafo (dirigido o no) finito. Podríamos entonces tomar como definición de grafo la de una matriz cuadrada con coeficientes en $\mathbb{N}$.

maxima 41:

```
(%i1)  load(graphs)$
(%i2)  g:cycle_graph(4)$
(%i3)  adjacency_matrix(g);
```

$$(\%o3)\quad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

```
(%i4)  h:from_adjacency_matrix(matrix([0,1,1],[1,0,1],[1,1,0]));
(%o4)  GRAPH(3 vertices, 3 edges)

(%i5)  print_graph(h);
Graph on 3 vertices with 3 edges.
Adjacencies:
2 : 1 0
1 : 2 0
0 : 2 1
(%o5)  done
```

El siguiente resultado nos muestra la importancia de las matrices de adyacencia.

Número de caminos entre dos vértices. Sea G un grafo cuyo conjunto de vértices es $\{v_1, v_2, \cdots, v_n\}$ y sea A su matriz de adyacencia. Entonces el coeficiente (i,j) de la matriz A^n es igual al número de caminos de longitud n que unen v_i con v_j.

maxima 42: Veamos como ejemplo los caminos en la rueda.

```
(%i1)  load(graphs)$
(%i2)  g:wheel_graph(3);
(%o2)  GRAPH(4vertices, 6edges)
(%i3)  a:adjacency_matrix(g);
```

$$(\%o3)\quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

```
(%i4)  a^^4;
```

$$(\%o4)\quad \begin{pmatrix} 21 & 20 & 20 & 20 \\ 20 & 21 & 20 & 20 \\ 20 & 20 & 21 & 20 \\ 20 & 20 & 20 & 21 \end{pmatrix}$$

Luego hay 20 caminos de longitud 4 para ir desde un vértice a otro distinto.
Podemos escribir una función que automatice esto.

```
(%i5)  caminos(grafo,longitud,i,j):=block(local(a),
       (a^^longitud)[i][j])$
(%i6)  caminos(g,4,1,2);
(%o6)  20
```

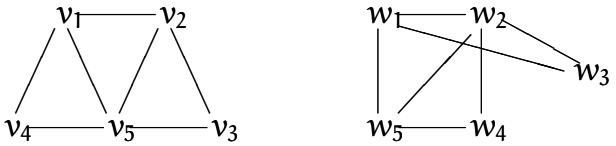
2.1. Matriz de incidencia. Sea G un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \cdots, v_n\}$ y cuyo conjunto de lados es $E = \{e_1, e_2, \cdots, e_m\}$. Se define la *matriz de incidencia* del grafo G como una matriz $n \times m$ que tiene en la posición (i,j) un 1 si $v_i \in f(e_j)$ y 0 en otro caso.

Observación:

1. Si tomamos otra ordenación de los vértices y/o lados, la matriz de incidencia puede ser diferente. En este caso, dos matrices de incidencia corresponden al mismo grafo si se puede pasar de una a otra mediante operaciones elementales por filas y/o columnas Tipo I (intercambio de filas y/o columnas).
2. El que un grafo tenga lados paralelos se traduce en que tenga dos columnas iguales en la matriz de incidencia, mientras que los lazos se traducen en filas con un único coeficiente "uno".
3. Si el grafo es dirigido, se puede definir también la matriz de incidencia. En este caso, el coeficiente (i,j) puede también tomar el valor -1 (si el lado e_j parte del vértice v_i). En tal caso, el grafo no podría tener lazos.

3. Isomorfismo de grafos

Consideremos los siguientes grafos

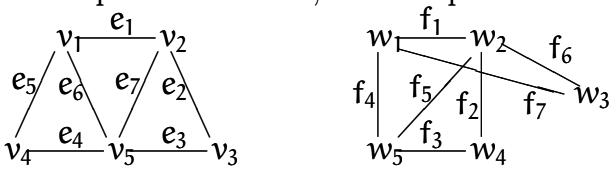


En una primera observación apreciamos dos grafos diferentes. Sin embargo, si profundizamos algo más encontramos muchas semejanzas entre ellos. Por ejemplo, ambos tienen igual número de vértices e igual número de lados. Existe un vértice en cada uno de ellos (v_5 en el primero y w_2 en el segundo) que está unidos al resto de vértices.

Siguiendo en esta línea, vemos que podemos renombrar los vértices del segundo grafo $w_1 \mapsto v'_1$, $w_2 \mapsto v'_5$, $w_3 \mapsto v'_4$, $w_4 \mapsto v'_3$ y $w_5 \mapsto v'_2$, y tenemos que por cada lado que une dos vértices v_i y v_j en el primer grafo tenemos un lado que une los vértices v'_i y v'_j en el segundo.

Vemos entonces que ambos grafos podemos considerarlos iguales. Lo único que los diferencia es el nombre que le hemos dado a los vértices (y a los lados) y la forma en que los hemos representado. Pero todo lo que digamos sobre un grafo es válido para el otro.

Para precisar un poco más lo que hemos hecho, vamos a ponerle nombre a los lados:



Entonces, lo que tenemos son dos biyecciones $h_V : V_G \to V_{G'}$ y $h_E : E_G \to E_{G'}$, que en este caso serían:

h_V	h_E
$v_1 \mapsto w_1$	$e_1 \mapsto f_4$
$v_2 \mapsto w_5$	$e_2 \mapsto f_3$
$v_3 \mapsto w_4$	$e_3 \mapsto f_2$
$v_4 \mapsto w_3$	$e_4 \mapsto f_6$
$v_5 \mapsto w_2$	$e_5 \mapsto f_7$
	$e_6 \mapsto f_1$
	$e_7 \mapsto f_5$

verificando que si $\gamma_G(e) = \{u, v\}$ entonces $\gamma_{G'}(h_E(e)) = \{h_V(u), h_V(v)\}$.

Nótese que en este caso, la aplicación h_V determina totalmente a la aplicación h_E.

Isomorfismo de grafos. Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos con aplicaciones de incidencia γ_G y $\gamma_{G'}$. Se dice que G y G' son isomorfos si existen dos biyecciones $h_V : V \to V'$ y $h_E : E \to E'$ tales que para cada lado $e \in E$ se verifica que $\gamma_{G'}(h_E(e)) = \{h_V(u), h_V(v)\}$ donde $\{u, v\} = \gamma_G(e)$.

En tal caso, diremos que las aplicaciones h_V y h_E forman un *isomorfismo* de G a G'.

Observación:

1. Si los grafos no tienen lados paralelos, entonces la aplicación h_V determina de forma única a la aplicación h_E. De ahí, que normalmente, para dar un isomorfismo de grafos se de únicamente como actúa sobre los vértices.
2. Si $h = (h_V, h_E)$ es un isomorfismo de G a G' entonces $((h_V)^{-1}, (h_E)^{-1})$ es un isomorfismo de G' a G.

En general, no es fácil determinar cuando dos grafos son isomorfos o no lo son. Claramente, si dos grafos son isomorfos deben tener igual número de vértices e igual número de lados. Sin

embargo, esto no es suficiente, como pone de manifiesto el siguiente ejemplo.

pues ambos tiene cuatro vértices y cuatro lados, y sin embargo no son isomorfos (¿por qué?).

Vemos que tenemos dos números asociados a cada grafo (número de vértices y número de lados) que deben coincidir para que los grafos sean isomorfos. Es lo que se llama *invariante por isomorfismo*. Obviamente, la coincidencia de estos números no implica que los grafos sean isomorfos.

Una propiedad se dice invariante por isomorfismo si dados dos grafos isomorfos G y G', uno satisface la propiedad si, y sólo si, la satisface el otro.

Grado de un vértice. Sea G un grafo y v un vértice de G. Se define el grado de v, y lo denotaremos como $\mathrm{gr}(v)$, como el número de lados (no lazos) de G que son incidentes en v más 2 veces el número de lazos incidentes en v.

Denotaremos por $D_k(G)$ como el número de vértices de V que tienen grado igual a k. A partir de esto, podemos construir la sucesión

$$D_0(G), D_1(G), D_2(G), \ldots, D_k(G), \ldots$$

que llamaremos *sucesión de grados*.

maxima 43: Veamos cómo son los grados de una rueda con cuatro radios.

```
(%i1) load(graphs)$
(%i2) g:wheel_graph(4);
(%o2) GRAPH(5 vertices, 8 edges)
(%i3) adjacency_matrix(g);
```

$$(\%o3)\quad \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

```
(%i4) makelist(vertex_degree(i,g),i,0,4);
(%o4) [3,3,3,3,4]
```

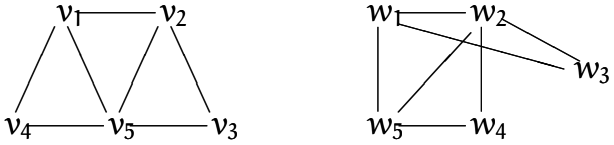
El vértice del centro tiene grado cuatro, mientras que los que están en la llanta tienen grado tres.

Nótese que si G es un grafo con n vértices $v_1, v_2, \ldots, v_n$ y l lados entonces

$$\mathrm{gr}(v_1) + \mathrm{gr}(v_2) + \cdots + \mathrm{gr}(v_n) = 2l,$$

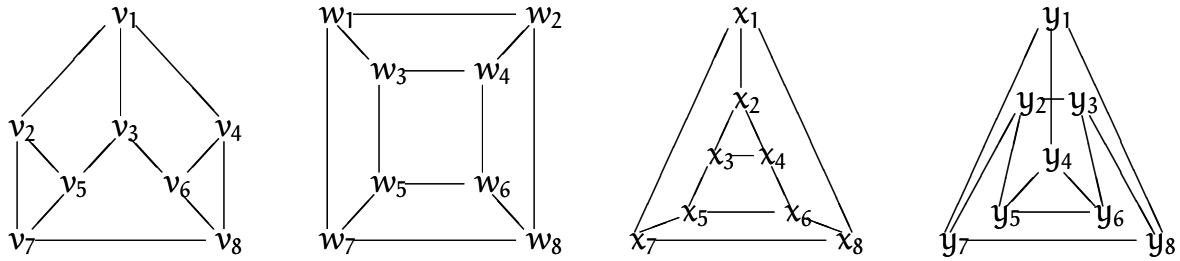
pues al contar todos los lados que inciden en todos los vértices (el miembro de la izquierda) estamos contando cada lado 2 veces (por cada uno de los vértices en los que incide)

Ejercicio 48: Calcula las sucesiones de grados para los siguientes grafos.



Es fácil comprobar que si $(h_V, h_E) : G \to G'$ es un isomorfismo de grafos y $v \in V$ entonces $gr(v) = gr(h_V(v))$, de donde deducimos que las sucesiones de grados de dos grafos isomorfos son iguales. El recíproco no es cierto, como podemos ver en el siguente ejemplo.

Consideramos los siguientes grafos:



En los cuatro grafos la sucesión de grados es la misma, pues todos los vértices tienen grado 3 (es decir, la sucesión de grados es en los cuatro casos $0, 0, 0, 8, 0, \ldots$). Sin embargo, el primero, tercero y cuarto son isomorfos y los isomorfismos vienen dados por

$$\begin{aligned}
v_1 &\mapsto x_5 \mapsto y_2\\
v_2 &\mapsto x_7 \mapsto y_7\\
v_3 &\mapsto x_6 \mapsto y_3\\
v_4 &\mapsto x_3 \mapsto y_5\\
v_5 &\mapsto x_8 \mapsto y_8\\
v_6 &\mapsto x_4 \mapsto y_6\\
v_7 &\mapsto x_1 \mapsto y_1\\
v_8 &\mapsto x_2 \mapsto y_4
\end{aligned}$$

mientras que el segundo no es isomorfo a ninguno de los otros tres, ya que en este segundo no hay ciclos de longitud 3, mientras que en los otros sí los hay ($v_2v_5v_7$ por ejemplo).

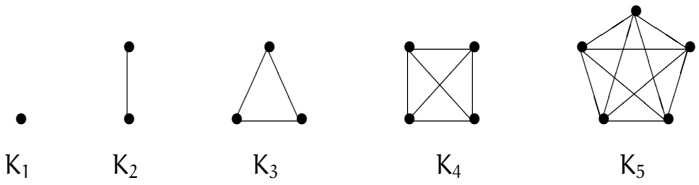
Los cuatro grafos que intervienen en este ejemplo tienen una peculiaridad, y es que todos los vértices tienen el mismo grado.

Grafos regulares. Un grafo es regular de grado n si todos sus vértices tienen grado igual a n.

Grafos completos. Se llama grafo completo de n vértices al grafo (con n vértices) que no tiene lazos ni lados paralelos, y dados dos vértices hay un lado que los une. Dicho de otra forma, su matriz de adyacencia toma el valor "cero" en todos los elementos de la diagonal y el valor "uno" en el resto.

Dicho grafo se suele denotar como K_n.

maxima 44: Los cinco primeros grafos completos son




```
(%i1)  load(graphs)$
(%i2)  makelist(adjacency_matrix(complete_graph(i)),i,1,5);
```

$$(\%o2)\quad \left[(0),\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix},\begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix},\begin{pmatrix}0&1&1&1&1\\1&0&1&1&1\\1&1&0&1&1\\1&1&1&0&1\\1&1&1&1&0\end{pmatrix}\right]$$

```
(%i3)  random_regular_graph(5,3);
```

$$(\%o3)\quad \mathrm{GRAPH}(6\mathrm{vertices}, 9\mathrm{edges})$$

```
(%i4)  adjacency_matrix(%);
```

$$(\%o4)\quad \begin{pmatrix}0&1&0&0&1&1\\1&0&1&1&0&0\\0&1&0&0&1&1\\0&1&0&0&1&1\\1&0&1&1&0&0\\1&0&1&1&0&0\end{pmatrix}$$

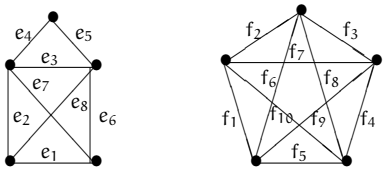
4. Grafos de Euler

Caminos y circuitos de Euler. Sea G un grafo conexo. Un camino de Euler es un recorrido en el que aparecen todos los lados.

Un circuito de Euler es un camino de Euler que es cerrado.

Un grafo con un circuito de Euler es un grafo de Euler.

Para los grafos



la sucesión $e_2e_4e_5e_8e_1e_7e_3e_6$ es un camino de Euler en el primer grafo, mientras que $f_1f_2f_3f_4f_5f_6f_8f_{10}f_7f_9$ es un circuito de Euler en el segundo.

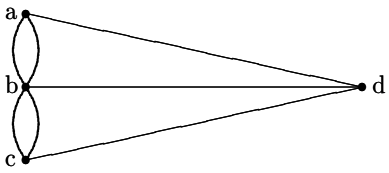
Caracterización de los grafos de Euler. Sea G un grafo conexo. Entonces

- G es un grafo de Euler si, y sólo si, el grado de cada vértice es par.
- G tiene un camino de Euler, si y sólo si G tiene exactamente dos vértices de grado impar (exactamente los vértices donde empieza y termina el camino).

La demostración se basa en este hecho:

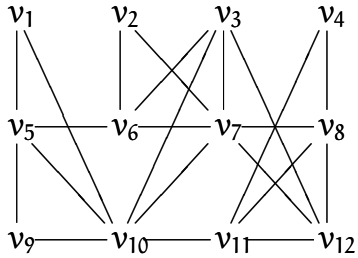
- Sea G un grafo en el que cada vértice tiene grado mayor que 1. Entonces G contiene un circuito (y por tanto un ciclo).

Ejercicio 49: Demuestra que en el grafo que representaba el problema de los puentes de Königsberg



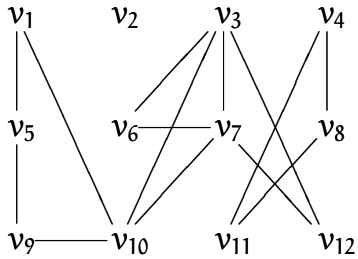
no existe ningún circuito de Euler. Por tanto, el problema de los puentes de Königsberg no tiene solución.

Consideramos el siguiente grafo

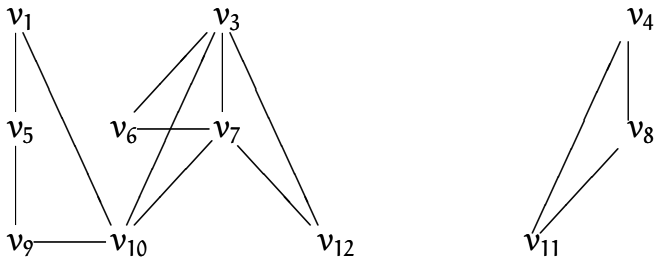


en el que vemos que los vértices v_1, v_2, v_4 y v_9 tienen grado 2; los vértices v_3, v_5, v_6, v_8, v_{11} y v_{12} tienen grado 4, mientras que los vértices v_7 y v_{10} tienen grado 6. Como todos los vértices tienen grado par, sabemos que existe un circuito de Euler. Vamos a encontrarlo.

Para esto, buscamos un circuito cualquiera, por ejemplo, $v_2v_6v_5v_{10}v_{11}v_{12}v_8v_7v_2$, y eliminamos los lados que intervienen en este circuito. Nos queda entonces el grafo



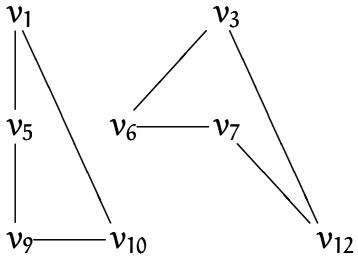
que tiene (aparte del vértice v_2) dos componentes conexas que son las siguientes:



de los cuales hemos de encontrar un circuito de Euler. En el segundo grafo, este circuito sería $v_4v_8v_{11}v_4$.

Vamos a encontrarlo en el primero. Para ello, hacemos como hicimos al principio.

Buscamos un circuito en dicho grafo, que podría ser $v_3v_7v_{10}v_3$; eliminamos los lados que intervienen, y nos queda entonces el grafo



que tiene dos componentes conexas. Para cada una de ellas es fácil encontrar un circuito de Euler. El circuito de la primera componente es $v_1v_5v_9v_{10}v_1$, mientras que el de la segunda es $v_3v_6v_7v_{12}v_3$.

Un vértice común entre los circuitos $v_3v_7v_{10}v_3$ y $v_1v_5v_9v_{10}v_1$ es v_{10}, mientras que un vértice común entre los circuitos $v_3v_7v_{10}v_3$ y $v_3v_6v_7v_{12}v_3$ podría ser v_3 (o v_7).

Recorremos entonces el circuito $v_3v_7v_{10}v_3$, y al llegar a los vértices que hemos elegido insertamos los circuitos de cada una de las componentes conexas.

$$v_3 \underbrace{v_6v_7v_{12}v_3} v_7v_{10} \underbrace{v_1v_5v_9v_{10}} v_3$$

Volvemos ya al grafo de partida. En él elegimos un circuito ($v_2v_6v_5v_{10}v_{11}v_{12}v_8v_7v_2$), que al eliminarlo dividía al grafo en dos componentes conexas. De cada una de éstas tomamos ahora un vértice común con el circuito. Sean éstos v_6 y v_{11}. Recorremos el circuito elegido, y al llegar a estos vértices insertamos los circuitos de Euler para cada una de las componentes. Tenemos entonces:

$$v_2v_6 \underbrace{v_7v_{12}v_3v_7v_{10}v_1v_5v_9v_{10}v_3v_6} v_5v_{10}v_{11} \underbrace{v_4v_8v_{11}} v_{12}v_8v_7v_2$$

que es un circuito de Euler para el grafo del que partíamos.

A continuación veremos un algoritmo que calcula, dado un grafo del que sabemos que tiene un camino o circuito de Euler, un tal camino.

Algoritmo de Fleury. Como entrada, tenemos un grafo G. Como salida, dos sucesiones S_V y S_E, que son las sucesiones de vértices y lados del camino buscado.

1. Si todos los vértices son de grado par, elegimos un vértice cualquiera v. Si G tiene dos vértices de grado impar elegimos uno de estos vértices.
2. Hacemos $S_V = v$ y $S_E = []$.
3. Si G tiene sólo a v, devuelve S_V y S_E, y termina.
4. Si hay un único lado e que incida en v, llamamos w al otro vértice donde incida el lado e; quitamos de G el vértice v y el lado e y vamos al paso 6.
5. Si hay más de un lado e que incida en v, elegimos uno de estos de forma que al quitarlo el grafo G siga siendo conexo. Llamamos e a dicho lado y w al otro vértice en el que incide e.
6. Añadimos w al final de S_V y e al final de S_E.
7. Cambiamos v por w y volvemos al paso 3.

5. Grafos de Hamilton

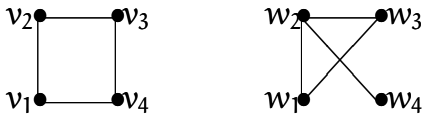
En la sección anterior estudiamos cuándo en un grafo podíamos encontrar un camino que recorriera todos los lados una sola vez. En esta, pretendemos estudiar como recorrer todos los vértices una sola vez.

Camino y circuito de Hamilton. Sea G un grafo. Un *camino de Hamilton* es un camino que recorre todos los vértices una sola vez.

Un *circuito de Hamilton* es un camino cerrado que recorre todos los vértices una sola vez (salvo los extremos).

Un grafo con un circuito de Hamilton se denomina *grafo de Hamilton* o *grafo hamiltoniano*.

maxima 45: Consideramos los siguientes grafos:



Entonces, el primer grafo es un grafo de Hamilton. Un circuito de Hamilton es $v_1v_2v_3v_4v_1$. Obviamente, al tener un circuito de Hamilton, podemos encontrar también un camino de Hamilton $(v_1v_2v_3v_4)$.

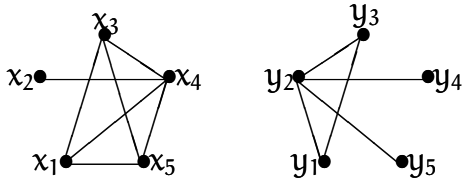
```
(%i1)  g1:cycle_graph(4)$
(%i2)  hamilton_cycle(g1);
(%o2)  [3,0,1,2,3]
```

En el segundo grafo tenemos un camino de Hamilton $(w_1w_3w_2w_4)$. Podemos ver como no existe ningún circuito de Hamilton, pues debería tener al menos dos lados incidentes en w_4 (el lado entrante y el lado saliente).

```
(%i3)  g2:from_adjacency_matrix(matrix(
       [0,1,1,0],[1,0,1,1],[1,1,0,0],[0,1,0,0]))$
(%i4)  hamilton_cycle(g2);
(%o4)  []

(%i5)  hamilton_path(g2);
(%o5)  [3,1,0,2]
```

Ejercicio 50: Determina si los siguientes grafos tienen caminos o circuitos de Hamilton.



Observaciones:

Puesto que a la hora de buscar un camino o circuito de Hamilton no podemos pasar dos veces por un mismo vértice, no es posible que el camino contenga dos lados paralelos, ni que contenga lazos. Supondremos por tanto en esta sección que todos los grafos que intervienen no tienen ni lazos ni lados paralelos.

Hemos visto en el ejemplo anterior, que si hay un vértice de grado 1, entonces el grafo no es de Hamilton.

Por otra parte, si un grafo con n vértices es de Hamilton, en el circuito de Hamilton intervienen n lados. Por tanto, un grafo de Hamilton con n vértices tiene al menos n lados.

Intuitivamente, cuantos más lados tenga un grafo con un número de vértices fijado, más fácil será poder encontrar un circuito de Hamilton.

6. Grafos bipartidos

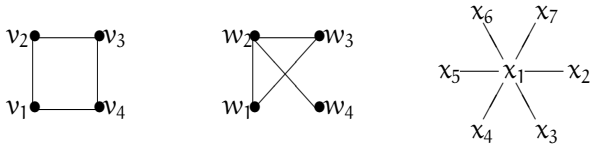
Grafo bipartido. Sea $G = (V, E)$ un grafo. Se dice que G es bipartido si podemos descomponer V en dos subconjuntos disjuntos V_1 y V_2 de forma que todo lado incide en un vértice de V_1 y en un vértice de V_2.

Un grafo $G = (V, E)$ se dice bipartido completo si es bipartido, y para cada $v_1 \in V_1$ y $v_2 \in V_2$ existe un único lado $e \in E$ tal que $\gamma_G(e) = \{v_1, v_2\}$.

Un grafo bipartido completo está completamente determinado por el cardinal de V_1 y V_2.

Si G es un grafo bipartido completo en el que V_1 tiene cardinal m y V_2 tiene cardinal n, entonces denotaremos a G como $K_{m,n}$.

maxima 46: Consideramos los siguientes grafos



Entonces el primer y el tercer grafos son bipartidos.

En el primero, se tiene que $V_1 = \{v_1, v_3\}$ y $V_2 = \{v_2, v_4\}$. Además, podemos ver que cualquier para cualquier pareja formada por un vértice de V_1 y un vértice de V_2 hay un lado y sólo uno que los une. Por tanto, es un grafo bipartido completo. Dado que V_1 y V_2 tienen dos elementos, dicho grafo es $K_{2,2}$.

```
(%i1)  load(graphs)$
(%i2)  g1:cycle_graph(4)$
(%i3)  is_bipartite(g1);
(%o3)  true
```

El segundo grafo no es bipartido. Para comprobarlo, supongamos que tenemos una división del conjunto de vértices de la forma $\{w_1, w_2, w_3, w_4\} = V_1 \cup V_2$. Entonces w_1 pertenecerá a uno de los dos conjuntos. Supongamos que a V_1. En tal caso, se tiene que $w_2 \in V_2$ (pues w_1 y w_2 están unidos por un lado) y $w_3 \in V_2$ (por el mismo motivo). Tenemos entonces dos vértices en el mismo subconjunto de la partición, y unidos por un lado.

```
(%i4)  g2:from_adjacency_matrix(matrix(
       [0,1,1,0],[1,0,1,1],[1,1,0,0],[0,1,0,0]))$
(%i5)  is_bipartite(g2);
(%o5)  false
```

En el tercero tenemos $V_1 = \{x_1\}$ y $V_2 = \{x_2, x_3, x_4, x_5, x_6, x_7\}$. Vemos también que este es un grafo bipartido completo, es decir, este grafo es $K_{1,6}$.

```
(%i6)  adjacency_matrix(complete_bipartite_graph(1,6));
```

$$(\%o6)\quad \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

El siguiente resultado nos da una caracterización de los grafos bipartidos.

Caraterización de grafos bipartidos. Sea $G = (V, E)$ un grafo. Entonces G es bipartido si, y sólo si, G no contiene ciclos de longitud impar.

Ejercicio 51: Sea G un grafo bipartido con partición V_1 y V_2. Supongamos que $|V_1| = n$ y $|V_2| = m$.

- Si G tiene un camino de Hamilton, entonces $|n - m| \leq 1$.

- Si G es un grafo de Hamilton, entonces $n = m$.
- Si G es completo y $|n - m| \leq 1$, entonces G tiene un camino de Hamilton.
- Si G es completo y $n = m$, entonces G es un grafo de Hamilton.

7. Grafos planos

En esta sección vamos a estudiar los grafos que pueden ser representados en el plano.

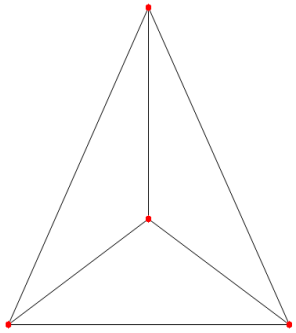
Representación plana. Sea G un grafo. Una representación de G se dice plana si los vértices y los lados se encuentran todos en un plano, y las líneas que representan dos lados distintos no se cortan.

Grafos planos. Un grafo se dice plano si admite una representación plana.

maxima 47:

```
(%i1)  load(graphs)$
(%i2)  is_planar(complete_graph(4));
(%o2)  true

(%i3)  draw_graph(complete_graph(4),redraw=true,program=planar_embedding);
```



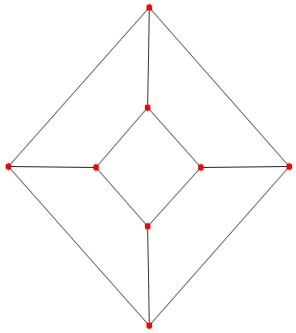
```
(%o3)  done
```

Cualquier poliedro tiene asociado un grafo. Los vértices son los vértices del poliedro, y los lados sus aristas. Este grafo es siempre plano.

Por ejemplo, el grafo correspondiente al tetraedro es K_4. El grafo correspondiente al cubo es

```
(%i4)  is_planar(cube_graph(3));
(%o4)  true

(%i5)  draw_graph(cube_graph(3),program=planar_embedding);
```



```
(%o5)  done
```

7.1. Caras. Una representación plana de un grafo divide al plano en que se encuentra en varias regiones, que denominaremos *caras*.

7.2. Característica de Euler. Sea G un grafo plano y conexo. Llamemos v al número de vértices, l al número de lados y c al número de caras de una representación plana. Entonces $v - l + c = 2$.

En general, si G es un grafo plano, y χ es el número de componentes conexas entonces $v-l+c = 1+\chi$.

En la representación plana que hicimos de K_4 se tienen un total de 4 caras. Como en K_4 se verifica que $v = 4$ y $l = 6$ entonces $v - l + c = 4 - 6 + 4 = 2$.

El cubo tiene 8 vértices, 12 aristas y 6 caras. Obviamente se ve que $v - l + c = 2$.

Vamos a demostrar aquí que sólo existen 5 sólidos regulares. Es decir, poliedros en donde todas las caras son polígonos regulares iguales.

Supongamos que tenemos un poliedro regular, y sea G el grafo asociado a dicho poliedro. Sabemos que se verifica que

$$v - l + c = 2$$

Sabemos además que este grafo es regular de grado r (r es el número de aristas que inciden en cada vértice) y que $r \geq 3$. Por tanto, se verifica que

$$rv = 2l.$$

Por otra parte, todas las caras son polígonos regulares de n lados. Si contamos el número de caras, y lo multiplicamos por n estamos contando el número de aristas dos veces, pues cada arista es arista común de dos caras. Por tanto, se tiene también que

$$nc = 2l.$$

Sustituyendo en la expresión $v - l + c = 2$ obtenemos que

$$\frac{2l}{r} - l + \frac{2l}{n} = 2 \Longrightarrow \frac{1}{r} + \frac{1}{n} = \frac{1}{2} + \frac{1}{l}$$

Sabemos que $r \geq 3$ y $n \geq 3$ (pues el polígono regular más simple es el triángulo). Si tanto n como r fueran simultáneamente mayores que 3, es decir, $n \geq 4$ y $r \geq 4$ tendríamos que $\frac{1}{n} \leq \frac{1}{4}$ y $\frac{1}{r} \leq \frac{1}{4}$, luego

$$\frac{1}{2} + \frac{1}{l} = \frac{1}{r} + \frac{1}{n} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \Longrightarrow \frac{1}{l} \leq 0,$$

lo cual es imposible.

Por tanto, tenemos dos posibilidades:

- $n = 3$. Las caras del sólido son triángulos.
  En este caso tenemos
  $$\frac{1}{3} + \frac{1}{r} = \frac{1}{2} + \frac{1}{l} \Longrightarrow \frac{1}{l} = \frac{1}{r} - \frac{1}{6} \Longrightarrow l = \frac{6r}{6-r}.$$
  Por tanto, $r < 6$, lo que nos da sólo tres posibilidades para r.
  1. $r = 3$. Entonces $l = \frac{6\cdot 3}{6-3} = 6$. Puesto que $nc = 2l$ deducimos que $c = 4$, y dado que $rv = 2l$ también tenemos que $v = 4$. El sólido regular resulta ser el tetraedro.
  2. $r = 4$. Aquí $l = \frac{24}{2} = 12$, y de aquí deducimos que $c = 8$ y $v = 6$. El sólido regular es el octaedro.
  3. $r = 5$. Ahora, $l = 30$, y por tanto $c = 20$ y $v = 12$. El sólido es el icosaedro.
- $r = 3$. Razonando igual que antes, pero intercambiando el papel de r y n tenemos tres posibilidades para n.
  1. $n = 3$. Este caso ya lo hemos analizado. Es el tetraedro.

2. $n = 4$. Ahora las caras son cuadrados. Ahora $l = 12$, lo que implica que $c = 6$ y $v = 8$. Estamos hablando del cubo.
3. $n = 5$. Las caras son pentágonos. Aquí $l = 30$, de donde $c = 12$ y $v = 20$. El sólido es en este caso el dodecaedro.

maxima 48:

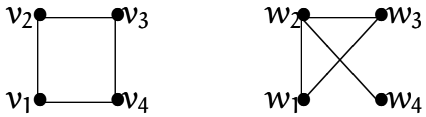
```
(%i1)  load(graphs)$
(%i6)  is_planar(complete_graph(5));
(%o6)  false

(%i7)  is_planar(complete_bipartite_graph(3,3));
(%o7)  false
```

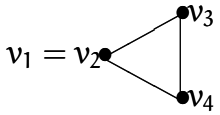
7.3. Contracción. Sea G un grafo. Una *contracción simple* de G es el resultado de identificar en G dos vértices adyacentes.

Una *contracción* de G es una cadena de contracciones simples.

Consideramos los grafos



Si en el primer grafo identificamos los vértices v_1 y v_2 obtenemos el grafo



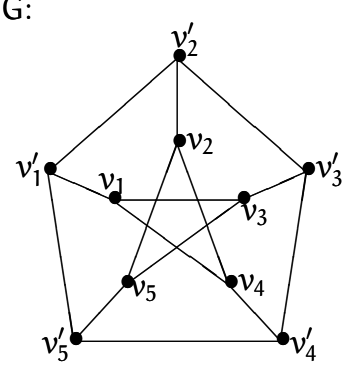
luego dicho grafo es una contracción del "cuadrado".

En el segundo grafo vamos a realizar una contracción simple identificando los vértices w_1 y w_2, y otra identificando w_2 y w_4. Los grafos que obtenemos son

Es muy intuitivo ver que cualquier contracción de un grafo plano sigue siendo un grafo plano.

Teorema de Kuratowski. Sea G un grafo. Entonces G es plano si, y sólo si, ningún subgrafo suyo puede contraerse a K_5 ni a $K_{3,3}$.

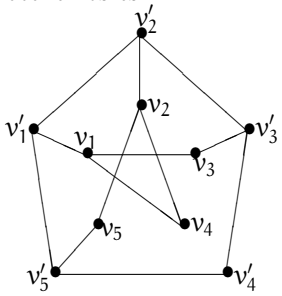
Consideramos el siguiente grafo G:



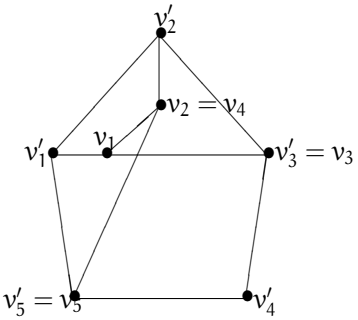
Entonces, si identificamos cada vértice v_i con v'_i (es decir, realizamos cinco contracciones) obtenemos el grafo K_5, que sabemos que no es plano. Deducimos por tanto que este grafo no es plano.

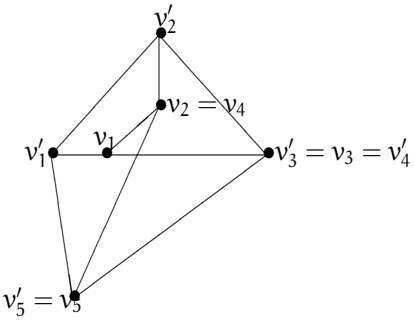
También podemos ver que este grafo no es plano como sigue:

Tomamos el subgrafo de G con los mismos vértices, y del que se eliminan los lados que unen v_3 con v_5, y v_4 con v'_4. El grafo que obtenemos es

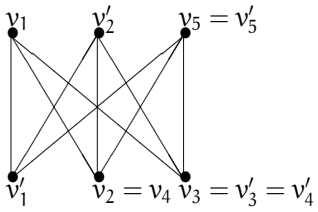


Identificamos los vértices v_2 con v_4, v_3 con v'_3 y v_5 con v'_5, y a continuación v'_4 con $v_3 = v'_3$. El grafo resultante es:





que podemos representar como



Es decir, hemos encontrado un subgrafo de G que puede contraerse hasta $K_{3,3}$.

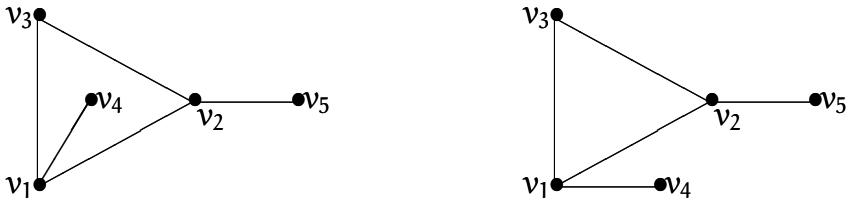
La representación que hemos obtenido de $K_{3,3}$ (no esta última) puede servirnos para comprobar que si en $K_{3,3}$ se suprime algún lado, el grafo resultante es plano (basta suprimir el lado v_2v_5 o el lado v_1v_3).

Por último, para acabar esta sección introducimos el concepto de grafo dual.

Grafo dual. Sea G un grafo plano. Supongamos que tenemos una representación plana con caras $c_1, c_2, \ldots, c_r$. Definimos el grafo dual para la representación dada como el grafo cuyo conjunto de vértices es igual al conjunto de caras (o tiene un vértice v'_i para cada cara c_i), y cuyo conjunto de lados coincide (o es biyectivo) con el conjunto de lados de G. En el grafo dual, un lado une dos vértices si en la representación plana de G dicho lado es frontera común de las dos caras.

Cuando hablamos de dual de un grafo, hacemos referencia a su representación plana. Esto es así porque el dual de un grafo depende de la representación plana que tomemos, como podemos ver en el siguiente ejemplo.

Vamos a considerar dos representaciones planas de un mismo grafo, y vamos a hallar el dual para cada una de las representaciones. El grafo tiene 5 vértices (v_1, v_2, v_3, v_4 y v_5) y 5 lados, de los que damos los dos vértices que unen (v_1v_2, v_1v_3, v_1v_4, v_2v_3 y v_2v_5). Dos representaciones planas del mismo grafo podrían ser:

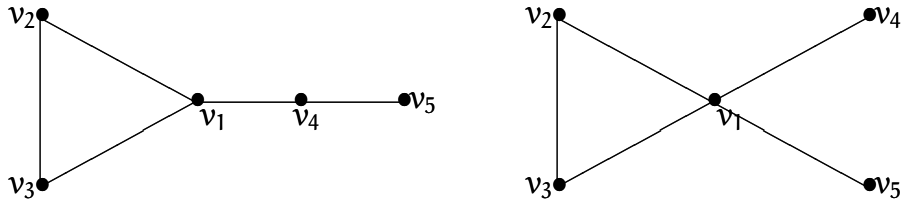


Calculamos el dual de cada una de las dos representaciones. Vemos que en ambos casos tenemos dos caras, lo que da lugar a 2 vértices en el grafo dual. Los grafos duales son entonces:

que podemos ver que no son isomorfos. Mientras el primer grafo tiene dos vértices de grado 5, el segundo tiene un vértice de grado 7 y uno de grado 3.

Del segundo grafo que hemos obtenido, podemos hacer varias representaciones planas. Por ejemplo,

y cada una de ellas tiene un dual diferente. En estos casos serían:



que no son isomorfos entre sí, ni isomorfos al grafo original (basta estudiar en cada caso la sucesión de grados).

Si quisiéramos obtener el grafo inicial, deberíamos tomar otra representación, aquella en la que uno de los lazos estaría "dentro" de la región c_2.

8. Coloración de grafos

8.1. Coloración. Sea $G = (V, E)$ un grafo. Una coloración G es una aplicación $f : V \to C$, donde C es un conjunto, de tal forma que para cualquier $e \in E$, si $\gamma_G(e) = \{v, w\}$ con $v \neq w$ entonces $f(u) \neq f(v)$.

Cuando el conjunto C sea un conjunto de colores, la aplicación f lo que hace es asignar un color a cada vértice de G, de forma que dos vértices adyacentes no tienen el mismo color.

Número cromático. Se llama número cromático de G, y lo representaremos como $\chi(G)$ al cardinal del menor conjunto C para el que existe una coloración de G.

maxima 49: El grafo •—• necesita al menos dos colores para colorearlo, ya que los dos vértices no pueden ser coloreados con el mismo color al ser adyacentes. Su número cromático es por tanto 2.

```
(%i1)  load(graphs)$
(%i2)  chromatic_number(path_graph(2));
(%o2)  2
```

En general, el número cromático del grafo K_n es n, pues todos los vértices deben tener colores distintos, ya que dos vértices cualesquiera son adyacentes.

```
(%i3)  makelist(chromatic_number(complete_graph(i)),i,1,15);
(%o3)  [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]
```

Si un grafo es plano, su número cromático es menor o igual que 4. Éste es un problema que se planteó por primera vez a mitad del siglo XIX, cuando se intentaba colorear los condados de un mapa de Inglaterra de forma que dos condados con frontera común tuvieran distinto color. El problema estuvo abierto durante más de un siglo, hasta que en 1976, Appel y Haken probaron el resultado basándose en un complicado análisis computacional.

El recíproco de este resultado no es cierto. $K_{3,3}$ tiene número cromático igual a 2, y sin embargo no es plano.

Ejercicio 52: Si G_1 es un subgrafo de G_2, entonces $\chi(G_1) \leq \chi(G_2)$.

Ejercicio 53: Demuestra que un grafo conexo es bipartido si y sólo si su número cromático vale 2.

En general, determinar el número cromático de un grafo es complicado. Para ello, vamos a valernos del polinomio cromático.

Polinomio cromático. Sea G un grafo y $x \in \mathbb{N}$. Vamos a denotar por $p(G,x)$ al número de coloraciones distintas, con x colores, que tiene el grafo G.

Observaciones

1. Si G es un grafo que tiene al menos un lado (que no es lazo) entonces $p(G,1) = 0$.
2. Si queremos colorear el grafo K_2 y disponemos de x colores, entonces para uno de los vértices podemos elegir cualquiera de los x colores, mientras que para el otro podemos elegir entre los $x-1$ restantes. El principio del producto nos dice entonces que $p(K_2,x) = x(x-1)$.
3. En general, se tiene que $p(K_n,x) = x(x-1)\cdots(x-n+1)$. De aquí se deduce que si $m \leq n$, $p(K_n,m) = 0$, mientras que $p(K_n,n) = n!$. Por tanto, el número cromatico de K_n es n.
4. Si G es un grafo cuyas componentes conexas son $G_1, G_2, \ldots, G_m$ entonces $p(G,x) = p(G_1,x)\cdot p(G_2,x)\cdots p(G_m,x)$.

   Por tanto, nos limitaremos a estudiar las coloraciones de los grafos conexos.
5. Si G es un grafo con n vértices, que es un camino simple, entonces $p(G,x) = x(x-1)^{n-1}$.

   Es decir, $G = (V,E)$ donde $V = \{v_1, v_2, \ldots, v_n\}$ y $E = \{e_1, e_2, \ldots, e_{n-1}\}$ y $\gamma_G(e_i) = \{v_i, v_{i+1}\}$.

   En este caso, para elegir una coloración de G con x colores, podemos elegir el que queramos para v_1, y para el resto de los vértices tenemos $x-1$ posibilidades (todas menos la que hayamos elegido para v_{i-1}). El principio del producto nos dice que $p(G,x) = x(x-1)^{n-1}$.

Antes de ver como calcular el polinomio cromático de un grafo, realizamos la siguiente construcción.

Dado un grafo G, tomamos un lado e (que no sea un lazo) que una los vértices u y v. Entonces el grafo G_e es el grafo con los mismos vértices que G, pero al que se le ha quitado el lado e, y el grafo G'_e es el grafo que resulta de identificar en G_e los vértices u y v.

Herramienta. Sea G un grafo, y u y v dos vértices adyacentes. Sea e el lado que los une. Entonces $p(G_e, x) = p(G, x) + p(G'_e, x)$.

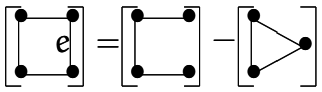
Esta expresión podemos verla como

$$p(G, x) = p(G_e, x) - p(G'_e, x),$$

lo cual nos permite reducir el cálculo del polinomio cromático de un grafo al cálculo de polinomios cromáticos más pequeños (con menos lados o con menos vértices). De esta forma, podemos reducirlo siempre al cálculo de polinomios cromáticos de grafos completos o de grafos que son caminos simples. Veamos algún ejemplo.

maxima 50: Para simplificar la notación, vamos a representar el polinomio cromático de un grafo encerrando el grafo entre corchetes.

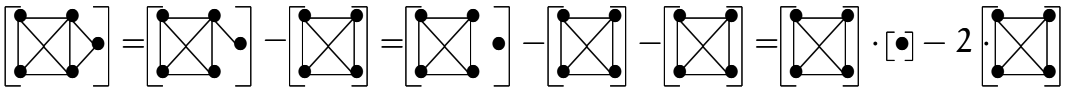
1. Vamos a calcular el polinomio cromático de un ciclo de longitud 4.



$$\begin{aligned} &= x(x-1)^3 - x(x-1)(x-2) \\ &= x(x-1)[x^2 - 2x + 1 - x + 2] \\ &= x(x-1)(x^2 - 3x + 3). \end{aligned}$$

```
(%i1)  load(graphs)$
(%i2)  chromatic_polynomial(cycle_graph(4),x);
(%o2)  (x-1)^3*x-(x-2)*(x-1)*x
(%i3)  factor(%);
(%o3)  (x-1)*x*(x^2-3*x+3)
```

2. Vamos a calcular otro polinomio cromático.



$$\begin{aligned} &= x(x-1)(x-2)(x-3)\cdot x - 2\cdot x(x-1)(x-2)(x-3) \\ &= x(x-1)(x-2)^2(x-3). \end{aligned}$$

```
(%i4)  g:complete_graph(4)$
(%i5)  add_vertex(4,g);
(%o5)  4
(%i6)  add_edges([[2,4],[3,4]],g);
(%o6)  done
(%i7)  chromatic_polynomial(g,x);
(%o7)  -x^4+3*x^3-2*x^2-(x-3)*(x-2)*(x-1)*x+(x-2)*(x-1)*x+(x-1)^4*x-
2*(x-1)^3*x+(x-1)^2*x
```


```
(%i8)  factor(%);
(%o8)  (x − 3) (x − 2)^2 (x − 1) x
```

9. Árboles

Comenzamos en esta sección el estudio de un tipo especial de grafos, los llamados árboles. Éstos fueron estudiados por vez primera por Kirchhoff, en 1847, en su trabajo de redes eléctricas. Sin embargo, estas estructuras son hoy día muy importantes en el estudio de las estructuras de datos, las ordenaciones, etc.

Árboles, bosques y árboles generadores. Un *árbol* es un grafo conexo que no tiene ciclos. Un grafo que no tenga ciclos se denomina *bosque*.

Dado un grafo conexo, un subgrafo suyo se dice *árbol generador* si tiene todos los vértices y es un árbol.

Nótese que un árbol no puede tener lazos ni lados paralelos.

Ejercicio 54: Sea G un grafo conexo que contiene un ciclo. Demuestra que si quitamos uno de los lados del ciclo el grafo sigue siendo conexo. Prueba, usando este hecho, que todo grafo conexo tiene un árbol generador

Ejercicio 55: Demuestra que todo árbol es un grafo plano.

Caracterizaciones de árboles. Sea G un grafo con n vértices, sin lados paralelos ni lazos. Entonces son equivalentes:

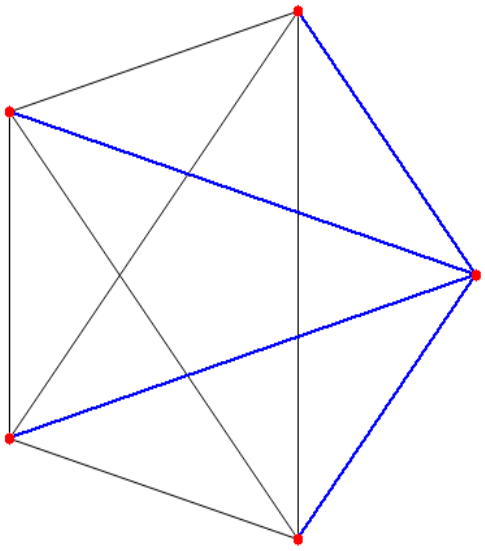
1. G es un árbol.
2. Dos vértices cualesquiera están unidos por un único camino simple.
3. G es conexo, pero si le quitamos un lado deja de serlo.
4. G no tiene ciclos, pero si le añadimos un lado tendrá algún ciclo.
5. G tiene $n - 1$ lados.

Es decir, los árboles son los menores grafos conexos, o los mayores grafos sin ciclos.

Nótese también que para las caracterizaciones segunda, tercera y cuarta no es necesario suponer que el grafo no tiene lazos ni lados paralelos, pues de ellas se deduce.

maxima 51:

```
(%i1)  load(graphs)$
(%i2)  g:complete_graph(5)$
(%i3)  a:minimum_spanning_tree(g)$
(%i5)  draw_graph(g,show_edges=edges(a));
```



Capítulo 7

Matrices con coeficientes en un cuerpo. Sistemas de ecuaciones lineales

Contenidos de este capítulo

1. Matrices

Sean $I = \{1, 2, \dots, m\}$ y $J = \{1, 2, \dots, n\}$. Una matriz de orden $m \times n$ sobre un cuerpo K es una aplicación

$$A : I \times J \to K, \ (i, j) \mapsto a_{ij}.$$

Normalmente a la matriz A la representaremos de la siguiente forma

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

y a veces simplemente escribiremos $A = (a_{ij})$, si queda claro dónde varían i y j. Diremos que A es una matriz con m filas y n columnas.

Denotaremos por $\mathcal{M}_{m\times n}(K)$ al conjunto de las matrices de orden $m \times n$ sobre K.

- $\mathcal{M}_{m\times n}(K)$ con la suma coordenada a coordenada tiene estructura de grupo abeliano, esto es, la suma es asociativa, tiene elemento neutro, toda matriz tiene inversa y es conmutativa.

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix}.$$

Ejercicio 56: Calcula suma de $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix}$ y $\begin{pmatrix} 2 & 3 & 3 \\ 3 & 0 & 2 \end{pmatrix}$ en $\mathcal{M}_{2\times 3}(\mathbb{Z}_5)$.

Sea $A = (a_{ij}) \in \mathcal{M}_{m\times n}(K)$ y $B = (b_{jk}) \in \mathcal{M}_{n\times p}(K)$. Entonces podemos definir el producto de A y B como $AB = C = (c_{ik}) \in \mathcal{M}_{m\times p}(K)$ con

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}.$$

Ejercicio 57: Sean $A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \end{pmatrix} \in \mathcal{M}_{2\times 3}$ y $B = \begin{pmatrix} 1 & 2 & 1 & 2 \\ 2 & 0 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_{3\times 4}$. Calcula AB.

Una matriz de orden $n \times n$ diremos que es una matriz cuadrada de orden n.

- $(\mathcal{M}_{n\times n}(K), +, \cdot)$ es un anillo.

Ejercicio 58: Sean $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$. Comprueba que $AB \neq BA$.

2. Determinantes

Dada $A = (a_{ij}) \in \mathcal{M}_{n\times n}(K)$, definimos $|A|$, el determinante de A, recursivamente de la siguiente forma.

1) Para $n = 1$, $|(a_{11})| = a_{11}$ (el determinante de una matriz de orden 1×1 es su único coeficiente).
2) Supuesto que sabemos calcular el determinante de matrices de orden $n-1$, dado $i \in \{1, \ldots, n\}$,

$$|A| = a_{i1}\alpha_{i1} + \ldots + a_{in}\alpha_{in},$$

donde $\alpha_{ij} = (-1)^{i+j}|A_{ij}|$ se conoce como el adjunto de la entrada a_{ij}, con $A_{ij} \in \mathcal{M}_{(n-1)\times(n-1)}(K)$ la matriz que se obtiene al eliminar la fila i-ésima y la columna j-ésima de A. Esta fórmula se conoce como Desarrollo de Laplace por la fila i del determinante de A, y el resultado no depende de i. Es más, también se puede desarrollar por cualquier columna. Dado j el Desarrollo de Laplace por la columna j es

$$|A| = a_{1j}\alpha_{1j} + \ldots + a_{nj}\alpha_{nj}.$$

Se puede comprobar fácilmente que

- $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$.
- $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{12}a_{21}a_{33}$.

Ejercicio 59: Calcula el determinante de $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}_7)$.

Ejercicio 60: Calcula el determinante de

$$\begin{pmatrix} 1 & 2 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 2 & 0 & 1 & 3 \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5).$$

Si $A = (a_{ij}) \in \mathcal{M}_{m\times n}(K)$, la matriz traspuesta de A es

$$A^t = \begin{pmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \ldots & a_{nm} \end{pmatrix} \in \mathcal{M}_{n\times m}(K),$$

esto es, la matriz que se obtiene a partir de A intercambiando filas por columnas.

Propiedades de los determinantes. Sea $A \in \mathcal{M}_{n\times n}(K)$.

1) $|A| = |A^t|$.
2) Si se intercambian dos filas (o dos columnas) de A se obtiene una nueva matriz cuyo determinante es $-|A|$.
3) Si multiplicamos todos los elementos de una fila (o de una columna) de A por $\alpha \in K$, obtenemos una matriz con determinante $\alpha|A|$.
4) Si a una fila de A le sumamos otra fila de A multiplicada por un elemento de K, entonces la nueva matriz tiene el mismo determinante que A (lo mismo ocurre si hacemos esta operación con columnas).
5) Si $B \in \mathcal{M}_{n\times n}(K)$, entonces $|AB| = |A||B|$.

Ejercicio 61: Calcula el determinante de la matriz

$$\begin{pmatrix} 2 & 3 & 4 & 0 \\ 3 & 1 & 2 & 2 \\ 4 & 3 & 3 & 1 \\ 2 & 3 & 3 & 2 \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{Z}_5).$$

El elemento neutro del producto en $\mathcal{M}_{n\times n}(K)$ es la matriz identidad, que es la matriz que tiene todas sus entradas cero salvo en la diagonal que tiene unos (cero es el elemento neutro de K para la suma, y uno el neutro para el producto). A dicha matriz la denotamos por I_n, o simplemente I cuando n queda claro en el contexto.

Una matriz $A \in \mathcal{M}_{n\times n}(K)$ es regular si tiene inversa para el producto, esto es, si existe B tal que $AB = BA = I_n$. En dicho caso, a la matriz B se le denota por A^{-1}.

La matriz adjunta de A es la matriz formada por los adjuntos de las entradas de A, a saber,

$$\overline{A} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{1} & a_{m2} & \dots & \alpha_{nn} \end{pmatrix}.$$

Teorema. Sea $A \in \mathcal{M}_{n\times n}(K)$. Entonces A es regular si y sólo si $|A| \neq 0$. En ese caso

$$A^{-1} = |A|^{-1}\overline{A}^t.$$

Ejercicio 62: Calcula la inversa de

$$\begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{Z}_3).$$

maxima 52: Vamos a ilustrar algunos ejemplos de operaciones con matrices en `maxima`.

```
(%i1) A:matrix([x,y],[z,t]);
```

(%o1)
$$\begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

```
(%i2) B:matrix([a,b],[c,d]);
```

(%o2) $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Hay que tener cuidado con la operación de producto, pues en `maxima` dicha operación se hace como en con la suma, entrada a entrada. Para efectuar el producto usamos el punto.

```
(%i3) A.B;
```

(%o3) $$\begin{pmatrix} cy+ax & dy+bx \\ az+ct & bz+dt \end{pmatrix}$$

```
(%i4) A*B;
```

(%o4) $$\begin{pmatrix} ax & by \\ cz & dt \end{pmatrix}$$

Lo mismo ocurre con la exponenciación.

```
(%i5) A^2;
```

(%o5) $$\begin{pmatrix} x^2 & y^2 \\ z^2 & t^2 \end{pmatrix}$$

```
(%i6) A^^2;
```

(%o6) $$\begin{pmatrix} yz+x^2 & xy+ty \\ xz+tz & yz+t^2 \end{pmatrix}$$

```
(%i7) determinant(A);
```

(%o7) $$tx-yz$$

```
(%i8) determinant(A.B)=determinant(A)*determinant(B);
```

(%o8) $$(cy+ax)\,(bz+dt)-(dy+bx)\,(az+ct)=(ad-bc)\,(tx-yz)$$

```
(%i9) expand(%);
```

(%o9) $$-adyz+bcyz+adtx-bctx=-adyz+bcyz+adtx-bctx$$

```
(%i10) is(%);
```

(%o10) $$\text{true}$$

```
(%i11) A^^-1;
```

(%o11) $$\begin{pmatrix} -\frac{t}{yz-tx} & \frac{y}{yz-tx} \\ \frac{z}{yz-tx} & -\frac{x}{yz-tx} \end{pmatrix}$$

```
(%i12) C:matrix([1,2,3],[4,5,6],[7,8,9]);
```

(%o12) $$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

```
(%i13) determinant(C);
```

(%o13) $$0$$

3. Operaciones elementales y determinantes

- Intercambio de filas: al intercambiar dos filas, el determinante cambia de signo.
- Sumarle a una fila un múltiplo de otra: el determinante en este caso permanece inalterado.
- Multiplicar un fila por un elemento λ no nulo: el determinante se multiplica por λ.

maxima 53: Para calcular determinantes a veces es más eficiente usar las operaciones que hemos visto anteriormente. Así efectuando operaciones elementales por filas o columnas (intercambio o suma por un factor de otra) podemos llegar a una matriz triangular superior, esto es, una matriz cuyas entradas por debajo de la diagonal son todas cero. A este proceso se le conoce como eliminación de Gauss-Jordan.

```
(%i14) triangularize(C);
```

(%o14)
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

El determinante de una matriz de esta forma es trivial, pues sólo se multiplican los valores de la diagonal.

maxima 54: Trabajemos ahora módulo 5.

```
(%i1)  modulus:5$
(%i2)  G:matrix([7,20],[16,47])$
(%i3)  H:rat(G);
```

(%o3)/R/
$$\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$$

```
(%i4)  determinant(H);
```

(%o4)/R/
$$-1$$

```
(%i5)  I:invert(H);
```

(%o5)/R/
$$\begin{pmatrix} -2 & 0 \\ 1 & -2 \end{pmatrix}$$

```
(%i6)  H.I;
```

(%o6)/R/
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

4. Forma normal reducida por filas (o columnas) de una matriz

Sea $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in \mathcal{M}_{m\times n}(K)$. El pivote de la fila i-ésima de A, si ésta tiene alguna entrada distinta de cero, es la primera entrada no nula de dicha fila, a saber, es $a_{ij} \neq 0$ con j mínimo verificando esa condición. Decimos que A está en forma normal reducida por filas (de forma análoga se define la forma normal por columanas) si

- Todas las filas nulas están debajo de las filas que tienen alguna entrada distinta de cero.
- Si a_{ij} es el pivote de la fila i-ésima, entonces $a_{ij} = 1$ y todas las demás entradas de su columna son cero.

- Siempre que a_{ij} sea el pivote de la fila i-ésima y a_{kl} es el pivote de la fila k-ésima, si $i < k$, entonces $j < l$.

Estas matrices tienen una forma escalonada, de forma que debajo de los escalones todas las entradas son cero, y encima del peldaño, que tiene que valer uno, también.

Dada una matriz A, siempre podemos calcular una forma normal reducida por filas (o por columnas) haciendo uso de las operaciones elementales que hemos visto anteriormente.

La forma normal reducida asociada a A es única, ya sea haciendo operaciones elementales por filas o por columnas.

maxima 55: Con el comando `echelon` podemos calcular una forma reducida escalonada, pero no es exactamente la forma reducida por filas de la matriz dada, ya que no se exige que encima del pivote hayan ceros.

```
(%i1) A:matrix([1,2,3,4],[5,6,7,8],[9,10,11,12])$
(%i2) echelon(A);
```

$$(\%o2)\quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

El comando `triangularize` da una forma reducida escalonada en la que los pivotes no tienen por qué ser uno.

```
(%i3) triangularize(A);
```

$$(\%o3)\quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Si quisiésemos calcular una transformación por columnas, basta que le apliquemos uno de estos comandos a la matriz traspuesta de la original, trasponiendo luego el resultado final.

```
(%i4) transpose(A);
```

$$(\%o4)\quad \begin{pmatrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{pmatrix}$$

```
(%i5) triangularize(%);
```

$$(\%o5)\quad \begin{pmatrix} 1 & 5 & 9 \\ 0 & -4 & -8 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

```
(%i6) transpose(%);
```

$$(\%o6)\quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 5 & -4 & 0 & 0 \\ 9 & -8 & 0 & 0 \end{pmatrix}$$

maxima 56: Podemos usar la forma normal reducida para calcular inversas.

```
(%i1) A:matrix([1,-1,1],[2,0,1],[0,3,-2])$
```

A esta matriz le añadimos la matriz identidad a la izquierda, donde gardaremos las operaciones elementales que se realizan con el comando `echelon`.


```
(%i2) M:echelon(addcol(A,ident(3)));
```

$$(\%o2)\quad \begin{pmatrix} 1 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 1 & -\frac{2}{3} & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 1 & -6 & 3 & -2 \end{pmatrix}$$

Las operaciones elementales las guardamos en una matriz que llamamos P.

```
(%i3) P:submatrix(M,1,2,3);
```

$$(\%o3)\quad \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{3} \\ -6 & 3 & -2 \end{pmatrix}$$

Como vemos, al multiplicar P por A, el resultado es una forma escalonada.

```
(%i4) T:P.A;
```

$$(\%o4)\quad \begin{pmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & -\frac{2}{3} \\ 0 & 0 & 1 \end{pmatrix}$$

Como hemos comentado antes, el comando `echelon` no hace ceros los elementos que están encima de los peldaños. Para conseguirlo, trasponemos la matriz, y repetimos el proceso.

```
(%i5) N:addcol(transpose(T),ident(3));
```

$$(\%o5)\quad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ \frac{1}{2} & -\frac{2}{3} & 1 & 0 & 0 & 1 \end{pmatrix}$$

```
(%i6) echelon(N);
```

$$(\%o6)\quad \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{2}{3} & 1 \end{pmatrix}$$

```
(%i7) Q:submatrix(%,1,2,3);
```

$$(\%o7)\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{1}{2} & \frac{2}{3} & 1 \end{pmatrix}$$

Ahora en P tenemos las operaciones necesarias para conseguir a partir de A una matriz triangular superior (eliminación de Gauss), y en Q^t las operaciones que eliminan los valores no nulos encima de los pivotes (eliminación Gauss-Jordan).

```
(%i8) paso:transpose(Q).P;
```

$$(\%o8)\quad \begin{pmatrix} 3 & -1 & 1 \\ -4 & 2 & -1 \\ -6 & 3 & -2 \end{pmatrix}$$

```
(%i9) paso.A;
```

$$(\%o9)\quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Por lo que la matriz `paso` es una inversa de A.

5. Rango de una matriz

Sea $A \in \mathcal{M}_{m\times n}(K)$. El rango de la matriz A es el número de filas no nulas de su forma normal reducida por filas. De forma análoga se define el rango por columnas de A.

Ejercicio 63: Calcula el rango por filas y por columnas de la matriz $\begin{pmatrix} 1 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 3}(\mathbb{Z}_5)$.

Teorema. El rango por filas de A coincide con el rango por columnas de A.
A dicha cantidad la llamaremos simplemente rango de A y la denotaremos por rango(A).

Teorema (rango y determinantes). El rango de una matriz es el máximo de los órdenes de sus submatrices cuadradas regulares.

Ejercicio 64: Calcula el rango de la matriz

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 1 & 3 & 1 \\ 4 & 5 & 5 & 1 \end{pmatrix} \in \mathcal{M}_{3\times 4}(\mathcal{R}).$$

maxima 57: El rango de una matriz también se puede calcular contando las filas no nulas de su forma triangular reducida asociada.

```
(%i1) A:matrix([0,1,2,3],[4,5,6,7],[8,9,10,11]);
```

(%o1)
$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{pmatrix}$$

```
(%i2) rank(A);
```

(%o2) 2

```
(%i3) echelon(A);
```

(%o3)
$$\begin{pmatrix} 1 & \frac{5}{4} & \frac{3}{2} & \frac{7}{4} \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```
(%i4) triangularize(A);
```

(%o4)
$$\begin{pmatrix} 4 & 5 & 6 & 7 \\ 0 & 4 & 8 & 12 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

6. Resolución de sistemas de ecuaciones lineales

Un sistema de ecuaciones lineales con n incógnitas sobre un cuerpo K es una expresión de la forma

$$\left.\begin{array}{c} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{array}\right\}.$$

Los elementos $a_{ij} \in K$ son los coeficientes del sistema, los $b_i \in K$ son los términos independientes, y las x_i son las incógnitas. Una solución es una n-upla $(s_1, \ldots, s_n) \in K^n$ tal que $x_1 = s_1, \ldots, x_n = s_n$ verifica las igualdades del sistema.

Las m igualdades del sistema anterior se pueden expresar como una única igualdad entre matrices,

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

a la que llamaremos expresión matricial del sistema. A dichas matrices se les llama matriz de coeficientes, matriz incógnita, y matriz de términos independientes.

La matriz ampliada del sistema es

$$\left(\begin{array}{ccc|c} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & \ddots & & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{array}\right).$$

Normalmente denotaremos a esta matriz por $(A|B)$.

Si un sistema tiene solución diremos que es compatible, y en caso contrario incompatible. Si tiene una única solución, es un sistema compatible determinado, y si tiene más de una solución decimos que es un sistema compatible indeterminado.

Dos sistemas de ecuaciones lineales sobre un cuerpo y con igual número de incógnitas son equivalentes si tienen las mismas soluciones.

Proposición (operaciones elementales).

1) Si intercambiamos de posición dos ecuaciones de un sistema, obtenemos un sistema equivalente.
2) Si multiplicamos una ecuación por un escalar no nulo, obtenemos un sistema equivalente.
3) Si a una ecuación le sumamos otra multiplicada por un escalar, también obtenemos un sistema equivalente al original.

Ejercicio 65: Resuelve el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_5$.

$$\left.\begin{array}{c} x_1 + x_2 + x_3 + x_4 = 1 \\ 2x_1 + 3x_2 + x_3 + x_4 = 2 \\ 4x_1 + 3x_2 + x_3 + 2x_4 = 0 \\ x_1 + x_2 + 2x_3 + 3x_4 = 2 \end{array}\right\}.$$

Teorema de Rouché-Frobenius. Sea $AX = B$ la expresión matricial de un sistema de ecuaciones lineales con n incógnitas.

1) El sistema es compatible si y sólo si $\text{rango}(A) = \text{rango}(A|B)$.
2) El sistema es compatible determinado si y sólo si $\text{rango}(A) = \text{rango}(A|B) = n$.

maxima 58: Vamos a estudiar el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_5$.

$$\left.\begin{array}{c} x+y+z=3 \\ 3x+y+2z=1 \\ x+4y=0 \end{array}\right\}.$$

```
(%i1)  modulus:5$
(%i2)  B:matrix([1,1,1],[3,1,2],[1,4,0])$
(%i3)  rank(B);
```
(%o3) 2

```
(%i4)  C:addcol(B,[3,1,0])$
(%i5)  rank(C);
```
(%o5) 2

El sistema es compatible determinado.

maxima 59: Estudiemos ahora el siguiente sistema con coeficientes en $\mathbb{Z}_7$ en función del parametro a.

$$\left.\begin{array}{c} x+y+z=a \\ 2x+ay+z=1 \\ 3x+3y+az=2 \end{array}\right\}.$$

```
(%i1)  modulus:7$
(%i2)  D:matrix([1,1,1],[2,a,1],[3,3,a])$
(%i3)  determinant(D);
```
(%o3) a^2-5a+6

```
(%i4)  factor(a^2-5*a+6);
```
(%o4) $(a-3)\,(a-2)$

Así, si $a \notin \{2,3\}$, la matriz de coeficientes tiene rango máximo y el sistema es compatible determinado.

Estudiemos por separado los casos $a=2$ y $a=3$.

```
(%i5)  E:subst(2,a,D);
```
(%o5)
$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 1 \\ 3 & 3 & 2 \end{pmatrix}$$

```
(%i6)  rank(E);
```
(%o6) 2

```
(%i7)  F:addcol(E,[2,1,2])$
(%i8)  rank(F);
```
(%o8) 3

Luego para $a=2$, el sistema es incompatible.

```
(%i9)  G:subst(3,a,D)$
(%i11) rank(G);
```
(%o11) 2

```
(%i12) H:addcol(G,[3,1,2])$
(%i13) rank(H);
```
(%o13) 2

Para $a = 3$ obtenemos un sistema compatible indeterminado.

Ejercicio 66: Estudia el siguiente sistema de ecuaciones con coeficientes en $\mathbb{Z}_5$.

$$\left.\begin{array}{c} 2x+4y+4z=1 \\ 3x+y+2z=2 \\ 4y+z=3 \end{array}\right\}.$$

Ejercicio 67: Estudia los siguientes sistemas con coeficientes en $\mathbb{R}$ en función de los parámetros a y b.

1)

$$\left.\begin{array}{c} ax+y+z=1 \\ x+y+z=2 \end{array}\right\},$$

2)

$$\left.\begin{array}{c} ax+y+z=1 \\ x+y+z=b \\ ax+by+z=1 \end{array}\right\},$$

3)

$$\left.\begin{array}{c} ax+y+z=1 \\ x-y+z=1 \end{array}\right\},$$

4)

$$\left.\begin{array}{c} ax+y+z=1 \\ x+2y+az=2 \end{array}\right\}.$$

maxima 60: El comando `linsolve` en máxima puede ser utilizado para resolver sistemas lineales de ecuaciones.

```
(%i1) linsolve([2*x+y+z=2,x-y-2*2=0],[x,y,z]);
```

$$(\%o1) \qquad [x=-\frac{\%r1-6}{3}, y=-\frac{\%r1+6}{3}, z=\%r1]$$

Como vemos, las soluciones dependen de un parámetro, que aquí se denomina %r1. El rango de la matriz de coeficientes es 2 como vemos a continuación, y es el máximo posible (sólo hay dos filas), por lo que coincide con el de la matriz ampliada. El sistema es compatible indeterminado.

```
(%i2) rank(matrix([2,1,1],[1,-1,-2]));
```

$$(\%o2) \qquad 2$$

Fórmula de Cramer. Un sistema es de Cramer si su matriz de coeficientes es cuadrada y regular. Si $AX = B$ es la expresión matricial de un sistema de Cramer, entonces el sistema es compatible determinado y su única solución es

$$|A|^{-1}(|M_1|, \ldots, |M_n|),$$

donde M_i es la matriz que se obtiene a partir de A cambiando la columna i-ésima por B.

Ejercicio 68: Prueba que el siguiente sistema de ecuaciones con coeficientes en $\mathbb{R}$ es un sistema de Cramer, y encuentra sus soluciones usando la fórmula de Cramer.

$$\left.\begin{array}{l} x+y+z=1 \\ x-y+z=0 \\ x+y-z=2 \end{array}\right\}.$$

Capítulo 8

Espacios vectoriales y aplicaciones lineales

Contenidos de este capítulo

1. Espacios y subespacios

Sea K un cuerpo. Diremos que un conjunto V tiene estructura de espacio vectorial sobre K si

1) en V hay una operación $+$ de forma que $(V,+)$ es un grupo abeliano,
2) existe una aplicación $K \times V \to V$, $(a, \overrightarrow{v}) \mapsto a\overrightarrow{v}$ verificando
   - I) $a(\overrightarrow{u}+\overrightarrow{v}) = a\overrightarrow{u} + a\overrightarrow{v}$,
   - II) $(a+b)\overrightarrow{u} = a\overrightarrow{u} + b\overrightarrow{u}$,
   - III) $a(b\overrightarrow{u}) = (ab)\overrightarrow{u}$,
   - IV) $1\overrightarrow{u} = \overrightarrow{u}$.

A los elementos de V los llamamos vectores y a los de K escalares. La aplicación descrita arriba se conoce como producto por escalares.

Ejercicio 69: Probar que si K es un cuerpo, entonces para cualesquiera enteros positivos n y m,

a) K^n,
b) $\{a(x) \in K[x] \text{ tales que } gr(a(x)) \leq n\}$,
c) $\mathcal{M}_{m\times n}(K)$,

son espacios vectoriales sobre K.

Ejercicio 70: Encuentra un espacio vectorial de cardinal 81.

Propiedades que se deducen de la definición.

1) $0\overrightarrow{u} = \overrightarrow{0}$ (el elemento neutro de $+$ en V).
2) $a\overrightarrow{0} = \overrightarrow{0}$.
3) Si $a\overrightarrow{u} = \overrightarrow{0}$, entonces $a = 0$ o $\overrightarrow{u} = \overrightarrow{0}$.
4) $-(a\overrightarrow{u}) = (-a)\overrightarrow{u} = a(-\overrightarrow{u})$.
5) $a(\overrightarrow{u}-\overrightarrow{v}) = a\overrightarrow{u} - a\overrightarrow{v}$.
6) $(a-b)\overrightarrow{u} = a\overrightarrow{u} - a\overrightarrow{u}$.
7) Si $a\overrightarrow{u} = a\overrightarrow{v}$ y $a \neq 0$, entonces $\overrightarrow{u} = \overrightarrow{v}$.

8) Si $a\vec{u} = b\vec{u}$ y $\vec{u} \neq \vec{0}$, entonces $a = b$.

En adelante V denotará un espacio vectorial sobre un cuerpo K.

Un subconjunto U de V es un subespacio vectorial de V si

1) $U \neq \emptyset$,
2) si $\vec{u}, \vec{v} \in U$, entonces $\vec{u} - \vec{v} \in U$ (U es un subgrupo de $(V,+)$),
3) si $a \in K$ y $\vec{u} \in U$, entonces $a\vec{u} \in U$.

Las dos últimas propiedades se pueden substituir por

2') si $\vec{u}, \vec{v} \in U$ y $a, b \in K$, entonces $a\vec{u} + b\vec{v} \in U$ (U es cerrado para combinaciones lineales de sus elementos).

Ejercicio 71: Demuestra que $\{(x,y,z) \in \mathbb{Q}^3$ tales que $x+y+z=0\}$ es un subespacio vectorial de $\mathbb{Q}^3$.

Ejercicio 72: Encuentra todos los elementos de $\{(x,y) \in \mathbb{Z}_3^2$ tales que $x+y=0\}$.

- Un subespacio vectorial de V es un espacio vectorial sobre K, con la misma suma y producto por escalares.
- La intersección de subespacios vectoriales de V es de nuevo un subespacio vectorial de V.

Sea S un subconjunto no vacío de V. El subespacio vectorial de V generado por S es la intersección de todos los subespacios vectoriales de V que contienen a S. A dicho subespacio lo denotaremos por $\langle S \rangle$.

- Si $S = \{\vec{u}_1, \ldots, \vec{u}_n\}$, entonces

$$\langle S \rangle = \{a_1\vec{u}_1 + \cdots + a_n\vec{u}_n \text{ tales que } a_1, \ldots, a_n \in K\}.$$

Ejercicio 73: Calcula todos los elementos del subespacio vectorial de $\mathbb{Z}_3^3$ generado por $\{(1,2,0),(0,1,2)\}$.

Sean $U_1, \ldots, U_n$ subespacios vectoriales de V. El subespacio vectorial suma de $U_1, \ldots, U_n$ es

$$U_1 + \ldots + U_n = \{\vec{u}_1 + \cdots + \vec{u}_n \text{ tales que } \vec{u}_1 \in U_1, \ldots, \vec{u}_n \in U_n\}.$$

- $U_1 + \cdots + U_n = \langle U_1 \cup \cdots \cup U_n \rangle$.
- Si $U_1 = \langle S_1 \rangle, \ldots, U_n = \langle S_n \rangle$, entonces $U_1 + \cdots + U_n = \langle S_1 \cup \cdots \cup S_n \rangle$.

Sean U y W subespacios vectoriales de V. Decimos que V es suma directa de U y W, y lo denotamos por $V = U \oplus W$, si todo vector $\vec{v} \in V$ se puede expresar de forma única como $\vec{v} = \vec{u} + \vec{w}$, con $\vec{u} \in U$ and $\vec{w} \in W$. En dicho caso, diremos que los subespacios vectoriales U y W son complementarios.

- $V = U \oplus W$ si, y sólo si, $V = U + W$ y $U \cap W = \{\vec{0}\}$.

Ejercicio 74: Sean $U = \{(x,y) \in \mathbb{R}^2$ tales que $x+y=0\}$ y $W = \{(x,y) \in \mathbb{R}^2$ tales que $x-y=0\}$. Demuestra que $\mathbb{R}^2 = U \oplus W$.

maxima 61: El conjunto K^n con K un cuerpo y n un entero positivo es un espacio vectorial. Para el caso $n=3$, el producto por escalares está definido así.

```
(%i1) a*[x,y,z];
```

$$(\%o1) \qquad [a\,x, a\,y, a\,z]$$

Y la suma de vectores se hace componente a componente.

```
(%i2) [x_1,y_2,z_3]+[x_2,y_2,z_2];
```

$$(\%o2) \qquad [x\_2 + x\_1, 2\,y\_2, z\_3 + z\_2]$$

Veamos que el conjunto de vectores de la forma $(x,y,0)$, con $x,y \in K$, es un subespacio de K^3.

```
(%i3) a*[x_1,y_1,0]+b*[x_2,y_2,0];
```

$$(\%o3) \qquad [b\,x\_2 + a\,x\_1, b\,y\_2 + a\,y\_1, 0]$$

Lo mismo ocurre con los de la forma (x,x,x).

```
(%i4) a*[x,x,x]+b*[x,x,x];
```

$$(\%o4) \qquad [b\,x + a\,x, b\,x + a\,x, b\,x + a\,x]$$

2. Bases

Un conjunto de vectores $S \subseteq V$ es linealmente dependiente si existen n un entero positivo, $\{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n\} \subseteq S$ y $(a_1, \ldots, a_n) \in K^n \setminus \{(0,\ldots,0)\}$ tales que $a_1\overrightarrow{v}_1 + \cdots + a_n\overrightarrow{v}_n = \overrightarrow{0}$. En caso contrario, decimos que S es un conjunto de vectores linealmente independientes.

Ejercicio 75: Demuestra que los vectores $(1,1,0),(0,1,1),(1,0,1) \in \mathbb{R}^3$ son linealmente independientes.

- S es un conjunto de vectores linealmente dependientes si y sólo si existe $\overrightarrow{v} \in S$ tal que $\overrightarrow{v} \in \langle S \setminus \{\overrightarrow{v}\}\rangle$.
- Si $\overrightarrow{0} \in S$, entonces S es un conjunto de vectores linealmente dependientes.
- Si S es un conjunto de vectores linealmente dependientes, entonces para todo $\overrightarrow{v} \in V$, $S \cup \{\overrightarrow{v}\}$ también es un conjunto de vectores linealmente dependientes.
- Si S, $\sharp S \geq 2$, es un conjunto de vectores linealmente independientes, entonces para todo $v \in S$ $S \setminus \{\overrightarrow{v}\}$ también es un conjunto de vectores linealmente independientes.

maxima 62: Veamos si $\{(1,2),(0,1)\}$ es un conjunto de vectores linealmente independientes en $\mathbb{Q}^2$.

```
(%i1) solve(x*[1,2]+y*[0,1],[x,y]);
```

$$(\%o1) \qquad [[x = 0, y = 0]]$$

Ahora probamos con $\{(1,2,3),(2,4,6)\}$ en $\mathbb{Q}^3$, y vemos que son dependientes.

```
(%i2) solve(x*[1,2,3]+y*[2,4,6],[x,y]);
```

solve: dependent equations eliminated: (2 3)

(%o2) $$[[x = -2\,\%r6, y = \%r1]]$$

Una base de V es un subconjunto S de vectores linealmente independientes de V tal que $V = \langle S \rangle$.

- Si $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ es una base de V, entonces para todo vector $\vec{v} \in V$, existen $a_1, \ldots, a_n \in K$ únicos tales que $\vec{v} = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$.

A la n-upla $(a_1, \ldots, a_n)$ se le llama coordenadas del vector $\vec{v}$ respecto de la base B.

Ejercicio 76: Demuestra que $B = \{(1,2),(1,3)\}$ es una base de $\mathbb{Z}_5^2$. Calcula las coordenadas del vector $(2,4)$ respecto de dicha base.

Teorema de la base. Todo espacio vectorial distinto de $\{\vec{0}\}$ tiene al menos una base. Además todas sus bases tienen el mismo cardinal.

Al cardinal de una base de V lo denotamos por $\dim(V)$, y nos referiremos a él como la dimensión de V.

Ejercicio 77: Prueba que $\dim(K^n) = n$, $\dim(\mathcal{M}_{m\times n}(K)) = nm$ y $\dim(\{a(x) \in K[x] \text{ tales que } gr(a(x)) \leq n\}) = n+1$.

Teorema de ampliación a base. Si $\dim(V) = n$ y $\{\vec{v}_1, \ldots, \vec{v}_m\}$ es un conjunto de vectores linealmente independientes de V, entonces $m \leq n$. Además existen $\vec{v}_{m+1}, \ldots, \vec{v}_n \in V$, de forma que $\{\vec{v}_1, \ldots, \vec{v}_m, \vec{v}_{m+1}, \ldots, \vec{v}_n\}$ es una base de V.

Ejercicio 78: Amplia $\{(1,1,1)\}$ una base de $\mathbb{R}^3$.

- Si $\dim(V) = n$, entonces cualquier conjunto de vectores de V linealmente independientes de cardinal n es una base de V.

Ejercicio 79: Prueba que $\{(1,2,1),(1,1,1),(1,0,0)\}$ es una base de $\mathbb{Z}_3^3$.

Ejercicio 80: Calcula una base del subespacio vectorial de $\mathbb{R}^3$ generado por $\{(1,2,1),(2,4,2),(1,3,2),(2,5,3)\}$.

maxima 63: Calculemos una base del subespacio vectorial U de $\mathbb{Q}^3$ generado por $\{(1,2,3),(1,1,1),(3,2,1)\}$.

```
(%i1) C:matrix([1,2,3],[1,1,1],[3,2,1]);
```

(%o1) $$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 3 & 2 & 1 \end{pmatrix}$$

Como las operaciones elementales por filas en la matriz C no alteran los sistemas de generadores,

```
(%i2) triangularize(C);
```

(%o2)
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

nos dice que $\{(1,2,3),(0,-1,-2)\}$ es una base de U.

maxima 64: Veamos que $B=\{(1,1,1),(1,2,1),(0,0,2)\}$ es una base de $\mathbb{Z}_5^3$, calculemos las coordenadas de $(2,3,4)$ respecto de esa base.

```
(%i1) modulus:5$
(%i2) solve(x*[1,1,1]+y*[1,2,1]+z*[0,0,2],[x,y,z]);
```
(%o2) $[[x=0,y=0,z=0]]$

Al ser tres generadores linealmente independientes en $\mathbb{Z}_5^3$, el conjunto dado es una base.

```
(%i3) solve(x*[1,1,1]+y*[1,2,1]+z*[0,0,2]-[2,3,4],[x,y,z]);
```
(%o3) $[[x=1,y=1,z=1]]$

maxima 65: Sean U y W los subespacios vectoriales de $\mathbb{Z}_5^3$ generados por $\{(1,1,1),(1,2,1)\}$ y $\{(1,2,3),(0,0,2)\}$, respectivamente. ¿Es $\mathbb{Z}_5^3=U+W$?

```
(%i1) modulus:5$
(%i2) D:matrix([1,1,1],[1,2,1],[1,2,3],[0,0,2]);
```
(%o2)
$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix}$$

```
(%i3) triangularize(D);
```
(%o3)
$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Así, una base para $U+W$ es $\{(1,1,1),(0,1,0),(0,0,2)\}$, por lo que $U+W=\mathbb{Z}_5^3$.

maxima 66: Sea U el subespacio vectorial de $\mathbb{Q}^3$ generado por $\{(1,1,1)(2,1,3),(4,3,5)\}$, calculemos un complementario de U.

Primero buscamos una base para U, aplicando operaciones elementales al sistema de generadores que nos dan.

```
(%i1) modulus:false$
(%i2) E:matrix([1,1,1],[2,1,3],[4,3,5])$
(%i3) triangularize(E);
```
(%o3)
$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Ahora probamos a añadir un vector que sea independiente con los dos anteriores.

```
(%i4) F:matrix([1,1,1],[0,-1,1],[1,0,0])$
```

```
(%i5)  triangularize(F);
```

(%o6)
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -2 \end{pmatrix}$$

De esta forma la recta generada por $(1,0,0)$ es un complemento de U en $\mathbb{Q}^3$.

maxima 67: Veamos ahora la dimensión del subespacio de $\mathbb{Z}_7^4$ generado por

$$\{(2,4,3,4),(4,1,6,1),(3,3,3,3),(5,0,6,0)\}.$$

```
(%i1)  modulus:7$
(%i2)  G:matrix([2,4,3,4],[4,1,6,1],[3,3,3,3],[5,0,6,0])$
(%i3)  triangularize(G);
```

(%o3)
$$\begin{pmatrix} -2 & 0 & -1 & 0 \\ 0 & -2 & -1 & -2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Luego la dimensión es dos, al tener dos filas no nulas en su forma reducida.

3. Ecuaciones del cambio de base

Sean $B = \{\vec{v}_1,\dots,\vec{v}_n\}$ y $B' = \{\vec{v}'_1,\dots,\vec{v}'_n\}$ dos bases de V. Sea $\vec{x} \in V$. Entonces existen $x_1,\dots,x_n,x'_1,\dots,x'_n \in K$ tales que $\vec{x} = x_1\vec{v}_1+\cdots+x_n\vec{v}_n$ y $\vec{x} = x'_1\vec{v}'_1+\cdots+x'_n\vec{v}'_n$. Queremos ver qué relación hay entre las coordenadas de $\vec{x}$ respecto de B y de B'. Para ello utilizaremos las coordenadas de los vectores de B respecto de B'. Supongamos que

$$\begin{aligned} \vec{v}_1 &= a_{11}\vec{v}'_1+\cdots+a_{1n}\vec{v}'_n, \\ &\vdots \\ \vec{v}_n &= a_{n1}\vec{v}'_1+\cdots+a_{nn}\vec{v}'_n. \end{aligned}$$

Entonces

$$\begin{aligned} \vec{x} = x_1\vec{v}_1+\cdots+x_n\vec{v}_n &= x_1(a_{11}\vec{v}'_1+\cdots+a_{1n}\vec{v}'_n)+\cdots+x_n(a_{n1}\vec{v}'_1+\cdots+a_{nn}\vec{v}'_n) \\ &= (x_1a_{11}+\cdots+x_na_{n1})\vec{v}'_1+\cdots+(x_1a_{1n}+\cdots+x_na_{nn})\vec{v}'_n = x'_1\vec{v}'_1+\cdots+x'_n\vec{v}'_n. \end{aligned}$$

Por tanto

$$\left.\begin{aligned} x'_1 &= x_1a_{11}+\cdots+x_na_{n1} \\ &\vdots \\ x'_n &= x_1a_{1n}+\cdots+x_na_{nn} \end{aligned}\right\},$$

que se conocen como las ecuaciones de cambio de base de B a B'. Éstas se pueden también expresar en forma matricial

$$(x'_1\dots x'_n) = (x_1\dots x_n)\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

A la matriz $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$ se le llama matriz de cambio de base de B a B'. Esta matriz es siempre regular y su inversa, A^{-1} es justamente la matriz de cambio de base de B' a B.

Ejercicio 81: Sean $B = \{(1,1,0),(1,2,1),(1,1,2)\}$ y $B' = \{(1,1,0),(1,0,1),(0,1,1)\}$ dos bases de $\mathbb{Z}_5^3$. Calcula las ecuaciones de cambio de base de B a B′.

maxima 68: Supongamos que K es $\mathbb{Z}_5$ y $V = \mathbb{Z}_5^2$.

```
(%i1) modulus:5;
```

$$(\%o1) \qquad 5$$

Elegimos dos bases, $B = \{\vec{v}_1, \vec{v}_2\}$ y $B' = \{\vec{u}_1, \vec{u}_2\}$.

```
(%i2) v1:[1,2];v2:[0,3];
```

$$(\%o2) \qquad [1,2]$$

$$(\%o3) \qquad [0,3]$$

```
(%i4) u1:[1,1];u2:[2,0];
```

$$(\%o4) \qquad [1,1]$$

$$(\%o5) \qquad [2,0]$$

Calculamos las coordenadas de $\vec{u}_1$ y $\vec{u}_2$ respecto de B.

```
(%i6) solve(a11*v1+a12*v2-u1,[a11,a12]);
```

$$(\%o6) \qquad [[a11 = 1, a12 = -2]]$$

```
(%i7) solve(a21*v1+a22*v2-u2,[a21,a22]);
```

$$(\%o7) \qquad [[a21 = 2, a22 = 2]]$$

Así la matriz de cambio de base de B′ a B es la siguiente.

```
(%i8) A:matrix([1,-2],[2,2]);
```

$$(\%o8) \qquad \begin{pmatrix} 1 & -2 \\ 2 & 2 \end{pmatrix}$$

El vector $\vec{u}_1 + \vec{u}_2$ tiene coordenadas $(1,1)$ en B′. Veamos cuáles son sus coordenadas en B.

```
(%i9) [1,1].A;
```

$$(\%o9) \qquad \begin{pmatrix} 3 & 0 \end{pmatrix}$$

Comprobamos el resultado.

```
(%i10) u1+u2=3*v1;
```

$$(\%o10) \qquad [3,1] = [3,6]$$

```
(%i11) mod(%,5);
```

$$(\%o11) \qquad [3,1] = [3,1]$$

La matriz de cambio de base de B a B′ es la inversa de A.

```
(%i12) A^^(-1);
```

(%o12) $$\begin{pmatrix} 2 & 2 \\ -2 & 1 \end{pmatrix}$$

maxima 69: Dadas las bases de $\mathbb{Q}^3$, $B = \{(1,2,3),(0,3,1),(0,0,4)\}$ y $B' = \{(1,1,1),(0,2,3),(0,0,7)\}$, veamos cuál es la matriz de cambio de base de B a B′ y la de B′ a B.

```
(%i1)  modulus:false$
(%i2)  solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[1,2,3],[x,y,z]);
```
(%o2) $[[x = 1, y = \frac{1}{2}, z = \frac{1}{14}]]$

```
(%i3)  solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[0,3,1],[x,y,z]);
```
(%o3) $[[x = 0, y = \frac{3}{2}, z = -\frac{1}{2}]]$

```
(%i4)  solve(x*[1,1,1]+y*[0,2,3]+z*[0,0,7]-[0,0,4],[x,y,z]);
```
(%o4) $[[x = 0, y = 0, z = \frac{4}{7}]]$

```
(%i5)  [x,y,z],%o2;
```
(%o5) $[1, \frac{1}{2}, \frac{1}{14}]$

```
(%i6)  [x,y,z],%o3;
```
(%o6) $[0, \frac{3}{2}, -\frac{1}{2}]$

```
(%i7)  [x,y,z],%o4;
```
(%o7) $[0, 0, \frac{4}{7}]$

La matriz de cambio de base de B a B′ es

```
(%i8)  H:matrix(%o5,%o6,%o7);
```
(%o8) $$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{14} \\ 0 & \frac{3}{2} & -\frac{1}{2} \\ 0 & 0 & \frac{4}{7} \end{pmatrix}$$

y la de B′ a B es

```
(%i9)  J:invert(%);
```
(%o9) $$\begin{pmatrix} 1 & -\frac{1}{3} & -\frac{5}{12} \\ 0 & \frac{2}{3} & \frac{7}{12} \\ 0 & 0 & \frac{7}{4} \end{pmatrix}$$

Si las coordenadas de un vector respecto de la base B son $(1,1,1)$, sus coordenadas respecto de B′ son

```
(%i10) [1,1,1].H;
```
(%o10) $$\begin{pmatrix} 1 & 2 & \frac{1}{7} \end{pmatrix}$$

4. Ecuaciones paramétricas de un subespacio vectorial

Supongamos que $\dim(V) = n$ y que U es un subespacio vectorial de V de dimensión r. Sea $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ una base de V, y $B_U = \{\vec{u}_1, \ldots, \vec{u}_r\}$ una base de U. Supongamos que

$$\begin{aligned} \vec{u}_1 &= a_{11}\vec{v}_1 + \cdots + a_{1n}\vec{v}_n, \\ &\vdots \\ \vec{u}_r &= a_{r1}\vec{v}_1 + \cdots + a_{rn}\vec{v}_n. \end{aligned}$$

Sea $\overrightarrow{x} = x_1\overrightarrow{v}_1 + \cdots + x_n\overrightarrow{v}_n$ un vector de V. Veamos qué tienen que verificar las coordenadas $(x_1, \ldots, x_n)$ para que $\overrightarrow{x} \in U$.

El vector $\overrightarrow{x} \in U$ si y sólo si existen $\lambda_1, \ldots, \lambda_r \in K$ tales que $\overrightarrow{x} = \lambda_1\overrightarrow{u}_1 + \cdots + \lambda_r\overrightarrow{u}_r$, y esto equivale a que

$$\begin{aligned}\overrightarrow{x} = \lambda_1(a_{11}\overrightarrow{v}_1 + \cdots + a_{1n}\overrightarrow{v}_n) + \cdots + \lambda_r(a_{r1}\overrightarrow{v}_1 + \cdots + a_{rn}\overrightarrow{v}_n)\\ = (\lambda_1 a_{11} + \cdots + \lambda_r a_{r1})\overrightarrow{v}_1 + \cdots + (\lambda_1 a_{1n} + \cdots + \lambda_r a_{rn})\overrightarrow{v}_n.\end{aligned}$$

Como las coordenadas son únicas,

$$\left.\begin{aligned} x_1 &= \lambda_1 a_{11} + \cdots + \lambda_r a_{r1}\\ &\vdots\\ x_n &= \lambda_1 a_{1n} + \cdots + \lambda_r a_{rn}\end{aligned}\right\}.$$

Estas ecuaciones son las ecuaciones paramétricas de U respecto de la base B.

Ejercicio 82: Dada la base $B = \{(1,1,0),(1,0,1),(0,1,1)$ de $\mathbb{Q}^3$, y U el subespacio vectorial de $\mathbb{Q}^3$ generado por $\{(1,2,1),(1,3,2),(2,5,3)\}$, calcula las ecuaciones paramétricas de U respecto de la base B.

maxima 70: Sea U el subespacio de $\mathbb{Z}_7^3$ generado por $\{(2,3,4),(2,4,4),(4,6,1)\}$, calculamos a continuación las ecuaciones paramétricas de U respecto de la base $B = \{(1,2,3),(0,3,4)(0,0,6)\}$.

Primero encontramos una base para U, y lo hacemos con el comando `triangularize`.

```
(%i1)  modulus:7$
(%i2)  K:matrix([2,3,4],[2,4,4],[4,6,1])$
(%i3)  triangularize(K);
```

$$(\%o3)\qquad \begin{pmatrix} 2 & 3 & -3\\ 0 & 2 & 0\\ 0 & 0 & 0\end{pmatrix}$$

Por tanto, U tiene como base $\{(2,3,-3),(0,2,0)\}$. Encontremos pues las coordenadas de sus elementos respecto de la base B.

```
(%i4)  solve(x*[1,2,3]+y*[0,3,4]+z*[0,0,6]-[2,3,-3],[x,y,z]);
```

$$(\%o4)\qquad [[x = 2, y = 2, z = 3]]$$

```
(%i5)  solve(x*[1,2,3]+y*[0,3,4]+z*[0,0,6]-[0,2,0], [x,y,z]);
```

$$(\%o5)\qquad [[x = 0, y = 3, z = -2]]$$

Así un elemento de coordenadas (x,y,z) respecto de la base B estará en U si y sólo si $(x,y,z) = \lambda(2,2,3) + \mu(0,3,5)$ para algún $\lambda, \mu \in \mathbb{Z}_7$. Las ecuaciones paramétricas son

$$\begin{cases} x = 2\lambda,\\ y = 2\lambda + 3\mu,\\ z = 3\lambda + 5\mu.\end{cases}$$

5. Aplicaciones lineales

En lo que queda de capítulo suponemos que V y V' son dos espacios vectoriales sobre el mismo cuerpo K.

Una aplicación $f : V \to V'$ es lineal (o un homomorfismo) si

1) para todo $\vec{u}, \vec{v} \in V$, $f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$,
2) para todo $a \in K$ y $\vec{v} \in V$, $f(a\vec{v}) = af(\vec{v})$.

- $f(\vec{0}) = \vec{0}$ (el primer $\vec{0}$ es de V y el segundo de V').
- $f(-\vec{v}) = -f(\vec{v})$.
- El núcleo de f, $N(f) = \{\vec{v} \in V$ tales que $f(\vec{v}) = \vec{0}\}$, es un subespacio vectorial de V.
- La imagen de f, $\mathrm{Im}(f)$, es un subespacio vectorial de V'.

Una aplicación lineal es un

1) monomorfismo si es inyectiva,
2) epimorfismo si es sobreyectiva,
3) isomorfismo si es biyectiva.

- Si f es un isomorfismo, también lo es f^{-1}.
- f es un monomorfismo si y sólo si $N(f) = \{\vec{0}\}$.
- Si $V = \langle\{\vec{v}_1, \ldots, \vec{v}_n\}\rangle$, entonces $\mathrm{Im}(f) = \langle\{f(\vec{v}_1), \ldots, f(\vec{v}_n)\}\rangle$.
- Si f es un monomorfismo y $\{\vec{v}_1, \ldots, \vec{v}_n\}$ son linealmente independientes, entonces $\{f(\vec{v}_1), \ldots, f(\vec{v}_n)\}$ también son linealmente independientes.

Ejercicio 83: Demuestra que $f : \mathbb{R}^3 \to \mathbb{R}^2$, $f(x, y, z) = (x+y, x+z)$ es una aplicación lineal. Calcula $N(f)$ y $\mathrm{Im}(f)$. ¿Es f un isomorfismo?

Ejercicio 84: Sea $f : \mathbb{Z}_7^2 \to \mathbb{Z}_7^3$, $(x, y, z) \mapsto (x, y, z + y)$. Calcula una base de $\mathrm{Im}(f)$. ¿Es f un epimorfismo?

Teorema: Las aplicaciones lineales vienen determinadas por la imagen de una base. Sea $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ una base de V, y $\{\vec{v}'_1, \ldots, \vec{v}'_n\} \subseteq V'$. Entonces existe una única aplicación lineal $f : V \to V'$ verificando que $f(\vec{v}_1) = \vec{v}'_1, \ldots, f(\vec{v}_n) = \vec{v}'_n$. Además, $\{\vec{v}'_1, \ldots, \vec{v}'_n\}$ es una base de V' si y sólo si f es un isomorfismo.

Los espacios vectoriales V y V' diremos que son isomorfos si existe un isomorfismo $f : V \to V'$.

- V y V' son isomorfos si y sólo si $\dim(V) = \dim(V')$.

Ejercicio 85: Sea U el subespacio vectorial de $\mathbb{Z}_5^3$ generado por $\{(1, 2, 3), (0, 1, 2), (1, 3, 0)\}$. Calcula el cardinal de U.

maxima 71: Sea $f : \mathbb{R}^3 \to \mathbb{R}^4$ definida por $f(x, y, z) = (x+y, x+z, 2x+y+z, y-z)$. Para calcular su núcleo usamos:

```
(%i1)  solve([x+y=0,x+z=0,2*x+y+z=0,y-z=0],[x,y,z]);
solve : dependentequationseliminated : (34)
(%o1)                          [[x = -%r1, y = %r1, z = %r1]]
```

Así $N(f) = \{(-a, a, a) \mid a \in \mathbb{R}\}$, que tiene como base a $\{(-1, 1, 1)\}$. Para calcular una base de la imagen, sabiendo que $\{f(1, 0, 0), f(0, 1, 0), f(0, 0, 1)$ es un sistema de generadores, hacemos lo siguiente.


```
(%i2)  f(x,y,z):=[x+y,x+z,2*x+y+z,y-z]$
(%i3)  A:matrix(f(1,0,0),f(0,1,0),f(0,0,1))$
(%i4)  triangularize(A);
```

$$(\%o4)\qquad \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto, una base de $\mathrm{Im}(f)$ es $\{(1,1,2,0),(0,-1,-1,1)\}$.

6. Ecuaciones de una aplicación lineal

Sea $f : V \to V'$ una aplicación lineal, y $B = \{\vec{v}_1,\dots,\vec{v}_n\}$ y $B' = \{\vec{v}'_1,\dots,\vec{v}'_m\}$ bases de V y V', respectivamente. Sean $\vec{x} = x_1\vec{v}_1+\cdots+x_n\vec{v}_n$ y $f(\vec{x}) = x'_1\vec{v}'_1+\cdots+x'_m\vec{v}'_m \in V'$. Queremos estudiar la relación que existe entre las coordenadas de $\vec{x}$ y $f(\vec{x})$.

Supongamos que

$$\begin{aligned} f(\vec{v}_1) &= a_{11}\vec{v}'_1+\cdots+a_{1m}\vec{v}'_m, \\ &\vdots \\ f(\vec{v}_n) &= a_{n1}\vec{v}'_1+\cdots+a_{nm}\vec{v}'_m. \end{aligned}$$

Entonces

$$\begin{aligned} f(\vec{x}) = f(x_1\vec{v}_1+\cdots+x_n\vec{v}_n) &= x_1f(\vec{v}_1)+\cdots+x_nf(\vec{v}_n) \\ &= x_1(a_{11}\vec{v}'_1+\cdots+a_{1m}\vec{v}'_m)+\cdots+x_n(a_{n1}\vec{v}'_1+\cdots+a_{nm}\vec{v}'_m) \\ &= (x_1a_{11}+\cdots+x_na_{n1})\vec{v}'_1+\cdots+(x_1a_{1m}+\cdots+x_na_{nm})\vec{v}'_m. \end{aligned}$$

Así

$$\left.\begin{aligned} x'_1 &= a_{11}x_1+\cdots+a_{n1}x_n \\ &\vdots \\ x'_m &= a_{1m}x_1+\cdots+a_{nm}x_n \end{aligned}\right\}$$

que se conocen como ecuaciones de la aplicación lineal respecto de las bases B y B'.

Estas ecuaciones se pueden expresar de forma matricial como

$$(x'_1\dots x'_m) = (x_1\dots x_n)\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}.$$

La matriz $A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix}$ es la matriz asociada a la aplicación lineal f respecto de las bases B y B'.

- f es un isomorfismo si y sólo si A es regular.

Ejercicio 86: Sea $f : \mathbb{Q}^2 \to \mathbb{Q}^3$, la aplicación lineal definida por $f(x,y,z) = (x,x+y,x-y)$. Calcula las ecuaciones de f respecto de las bases $\{(1,1),(1,2)\}$ de $\mathbb{Q}^2$ y $\{(1,1,0),(1,0,1),(0,1,1)\}$ de $\mathbb{Q}^3$.

Ejercicio 87: Sea $f : \mathbb{Z}_7^2 \to \mathbb{Z}_7^3$ una aplicación lineal tal que $f(1,2) = (2,3,1)$ y $f(2,5) = (3,4,2)$. Calcula la expresión general $f(x,y)$.

Ejercicio 88: Encuentra la matriz asociada a la base $\{(1,0,0),(0,1,0),(0,0,1)\}$ de una aplicación lineal $f:\mathbb{R}^3\to\mathbb{R}^3$ que verifica que $(1,0,0)\in N(f)$ y $\mathrm{Im}(f)=\langle\{(2,3,1),(3,3,2)\}\rangle$.

maxima 72: Calculemos la expresión matricial de la aplicacion lineal del ejemplo anterior respecto de las bases $B=\{(1,1,0),(1,0,1),(0,1,1)\}$ y $B'=\{(1,1,1,1),(0,1,1,1),(0,0,1,1),(0,0,0,1)\}$. Podemos por ejemplo calcular las coordenadas de las imágenes por f de los elementos de B respecto de B'.

```
(%i1) f(x,y,z):=[x+y,x+z,2*x+y+z,y-z]$
(%i2) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
      f(1,1,0),[x,y,z,t]);
```

$$(\%o2)\qquad [[x=2,y=-1,z=2,t=-2]]$$

```
(%i3) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
      f(1,0,1),[x,y,z,t]);
```

$$(\%o3)\qquad [[x=1,y=1,z=1,t=3]]$$

```
(%i4) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]+t*[0,0,0,1]-
      f(0,1,1),[x,y,z,t]);
```

$$(\%o4)\qquad [[x=1,y=0,z=1,t=-2]]$$

```
(%i5) C:matrix([2,-1,2,-2],[1,1,1,-4],[1,0,1,-2]);
```

$$(\%o5)\qquad \begin{pmatrix}2&-1&2&-2\\1&1&1&-4\\1&0&1&-2\end{pmatrix}$$

Por tanto la expresión matricial es $(x',y',z',t')=(x,y,z)C$.

maxima 73: Tomamos una base $B=\{\vec{v}_1,\vec{v}_2,\vec{v}_3\}$ en $\mathbb{Q}^3$.

```
(%i1) v1:[1,2,1];v2:[1,1,0];v3:[0,0,3];
```

$$(\%o1)\qquad [1,2,1]$$

$$(\%o2)\qquad [1,1,0]$$

$$(\%o3)\qquad [0,0,3]$$

Y las imágenes de esos vectores respecto de la base usual $\{(1,0),(0,1)\}$ en $\mathbb{Q}^2$.

```
(%i4) fv1:[1,1];fv2:[2,1];fv3:[1,2];
```

$$(\%o4)\qquad [1,1]$$

$$(\%o5)\qquad [2,1]$$

$$(\%o6)\qquad [1,2]$$

La matriz de f asociada a dichas bases es:

```
(%i7) A:matrix(fv1,fv2,fv3);
```

(%o7) $$\begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}$$

Si queremos calcular la imagen de un elemento con coordenadas (x,y,z) respecto de B, sólo tenemos que multiplicar esas coordenadas por A.

```
(%i8) [x,y,z].A;
```

(%o8) $$\begin{pmatrix} z+2y+x & 2z+y+x \end{pmatrix}$$

Así $f(x,y,z) = (x+2y+z, x+y+2z)$, donde (x,y,z) son coordenadas respecto de B.

Si lo que queremos es la expresión de $f(x,y,z)$, con (x,y,z) coordenadas respecto de la base usual $\{(1,0,0),(0,1,0),(0,0,1)\}$, lo que hacemos es calcular primero el cambio de base de B a la base usual, y luego lo multiplicamos por A, obteniendo así la expresión matricial respecto de las bases usuales.

```
(%i9) B:matrix(v1,v2,v3);
```

(%o9) $$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

```
(%i10) B^^-1;
```

(%o10) $$\begin{pmatrix} -1 & 2 & \frac{1}{3} \\ 1 & -1 & -\frac{1}{3} \\ 0 & 0 & \frac{1}{3} \end{pmatrix}$$

```
(%i11) AA:%.A;
```

(%o11) $$\begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ -\frac{4}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

Veamos que el resultado es el deseado ($\overrightarrow{v}_i$ lo definimos en función de la base usual).

```
(%i12) v1.AA;v2.AA;v2.AA
```

(%o12) $$\begin{pmatrix} 1 & 1 \end{pmatrix}$$

(%o13) $$\begin{pmatrix} 2 & 1 \end{pmatrix}$$

(%o14) $$\begin{pmatrix} 1 & 2 \end{pmatrix}$$

Por tanto las coordenadas de $f(x,y,z)$ respecto de la base usual de $\mathbb{Q}^2$, con (x,y,z) coordenadas en la base usual de $\mathbb{Q}^3$, la podemos calcular como sigue.

```
(%i17) [x,y,z].AA;
```

(%o17) $$\begin{pmatrix} \frac{z}{3} - \frac{4y}{3} + \frac{10x}{3} & \frac{2z}{3} - \frac{2y}{3} + \frac{5x}{3} \end{pmatrix}$$

maxima 74: Calculemos la expresión de una aplicación lineal $g : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ tal que $g(1,1,1) = (2,0)$, $g(1,2,1) = (1,1)$ y $g(0,0,2) = (3,3)$.

```
(%i1)  modulus:5$
(%i2)  D:matrix([1,1,1],[1,2,1],[0,0,2])$
(%i3)  E:invert(D)$
```

```
(%i4)  F:rat(E);
```

$$(\%o4)/R/ \qquad \begin{pmatrix} 2 & -1 & 2 \\ -1 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Tenemos así las coordenadas de los vectores $(1,0,0)$, $(0,1,0)$ y $(0,0,1)$ respecto de la base $\{(1,1,1),(1,2,1),(0,0,2)\}$.

```
(%i5)  G:matrix([2,0],[1,1],[3,3])$
```

Y sus imágenes por g se calculan multiplicando por G.

```
(%i6)  H:F.G;
```

$$(\%o6)/R/ \qquad \begin{pmatrix} -1 & 0 \\ -1 & 1 \\ -1 & -1 \end{pmatrix}$$

Por tanto $g(x,y,z) = (4x+4y+4z, y+4z)$. Comprobemos si hemos hecho bien los cálculos.

```
(%i7)  g(x,y,z):=[4*x+4*y+4*z,y+4*z]$
(%i8)  rat(g(1,1,1));
```

$$(\%o8)/R/ \qquad [2,0]$$

```
(%i9)  rat(g(1,2,1));
```

$$(\%o9)/R/ \qquad [1,1]$$

```
(%i10) rat(g(0,0,2));
```

$$(\%o10)/R/ \qquad [-2,-2]$$

7. Espacio vectorial cociente

Sea U un subespacio vectorial de V. Definimos en V la siguiente relación de equivalencia: $\overrightarrow{x}\ R\ \overrightarrow{y}$ si $\overrightarrow{x} - \overrightarrow{y} \in U$. Denotamos por $\frac{V}{U}$ al conjunto cociente $\frac{V}{R}$.

- El conjunto $\frac{V}{U}$ es un espacio vectorial con las operaciones $[\overrightarrow{x}] + [\overrightarrow{y}] = [\overrightarrow{x} + \overrightarrow{y}]$ y $k[\overrightarrow{x}] = [k\overrightarrow{x}]$. A dicho espacio vectorial se le conoce como espacio vectorial cociente de V sobre U.
- Si $\{\overrightarrow{u}_1, \ldots, \overrightarrow{u}_m\}$ es una base de U y la ampliamos a una base de V, $\{\overrightarrow{u}_1, \ldots, \overrightarrow{u}_m, \overrightarrow{u}_{m+1}, \ldots, \overrightarrow{u}_n\}$, entonces $\{[\overrightarrow{u}_{m+1}], \ldots, [\overrightarrow{u}_n]\}$ es una base de $\frac{V}{U}$. Así

$$\dim\left(\frac{V}{U}\right) = \dim(V) - \dim(U).$$

Primer teorema de isomorfía. Si $f : V \to V'$ es una aplicación lineal, entonces los espacios vectoriales $\frac{V}{N(f)}$ e $\mathrm{Im}(f)$ son isomorfos (el isomorfismo viene dado por $[\overrightarrow{v}] \mapsto f(v)$).

- $\dim(V) = \dim(N(f)) + \dim(\mathrm{Im}(f))$.

Ejercicio 89: Sea $f : \mathbb{R}^3 \to \mathbb{R}^2$ definida por $f(x,y,z) = (2x+y, 3x+z)$. Encuentra una base de $N(f)$.

Segundo teorema de isomorfía. Si U_1 y U_2 son subespacios de V, entonces los espacios vectoriales $\frac{U_2}{U_1\cap U_2}$ y $\frac{U_1+U_2}{U_1}$ son isomorfos.

- $\dim(U_1)+\dim(U_2)=\dim(U_1+U_2)+\dim(U_1\cap U_2)$.

Ejercicio 90: Dados los subespacios vectoriales de $\mathbb{Z}_5^3$, $U=\langle\{(1,1,2),(1,2,3)\}\rangle$ y $W=\langle\{(1,0,0),(2,1,3)\}\rangle$, calcula la dimensión de $U\cap W$.

Ejercicio 91: Sea U el subespacio vectorial de $\mathbb{Q}^3$ generado por $\{(1,2,1)\}$. Calcula un complementario de U.

maxima 75: Sea U el subespacio vectorial de $\mathbb{Q}^4$ generado por $\{(1,1,1,1),(1,2,3,4),(1,0,-1,-2)\}$, calculemos una base del espacio cociente $\mathbb{Q}^4/U$.

```
(%i1)  A:matrix([1,1,1,1],[1,2,3,4],[1,0,-1,-2])$
(%i2)  triangularize(A);
```

$$(\%o2)\qquad \begin{pmatrix}1&0&-1&-2\\0&2&-1&1\\0&0&0&0\end{pmatrix}$$

Una base de U es {(1,0,-1,-2),(0,2,4,6)}. Ahora la ampliamos a una base de $\mathbb{Q}^4$.

```
(%i3)  B:matrix([1,0,-1,-2],[0,2,4,6],[0,0,1,0],[0,0,0,1])$
(%i4)  determinant(B);
```

$(\%o4)\quad 2$

Una base del cociente es $\{[(0,0,1,0)],[(0,0,0,1)]\}$.

maxima 76: Sea $f:\mathbb{Q}^4\to\mathbb{Q}^3$ definida por

```
(%i1)  f(x,y,z,t):=[x+y+z,x+z+t,y-t]$
```

Como

```
(%i2)  triangularize(matrix(f(1,0,0,0),f(0,1,0,0),f(0,0,1,0),f(0,0,0,1)));
```

$$(\%o2)\qquad \begin{pmatrix}1&1&0\\0&-1&1\\0&0&0\\0&0&0\end{pmatrix}$$

deducimos que la imagen de f tiene dimensión 2. Por el primer teorema de isomorfía, su núcleo debería también tener dimensión dos. Comprobémoslo:

```
(%i3)  solve(f(x,y,z,t),[x,y,z,t]);
```

solve : dependentequationseliminated : (1)

$(\%o3)\quad [[x=-\%r3-\%r2,y=\%r2,z=\%r3,t=\%r2]]$

maxima 77: Sean U y W los subespacios de $\mathbb{Z}_7^4$ generados por $\{(1,0,1,0),(1,2,1,2),(1,5,1,5)\}$ y $\{(2,3,4,0),(1,5,2,0),(2,3,2,3)\}$, respectivamente. Veamos cuál es la dimensión de $U\cap W$.

Un sistema de generadores para $U+W$ es $\{(1,0,1,0),(1,2,1,2),(1,5,1,5),(2,3,4,0),(1,5,2,0),(2,3,2,3)\}$.

```
(%i1)  modulus:7$
```

Las dimensiones de U y W son dos, ya que

```
(%i2) triangularize(matrix([1,0,1,0],[1,2,1,2],[1,5,1,5]));
```

$$(\%o2)\qquad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

y

```
(%i3) triangularize(matrix([2,3,4,0],[1,5,2,0],[2,3,2,3]));
```

$$(\%o3)\qquad \begin{pmatrix} 2 & 3 & -3 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Por último,

```
(%i4) triangularize(matrix([1,0,1,0],[1,2,1,2],[1,5,1,5],[2,3,4,0],[1,5,2,0],[2,3,2,3]));
```

$$(\%o4)\qquad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Esto nos dice que la dimensión de $U+W$ es 3. Por el Segundo Teorema de Isomorfía, deducimos que la dimensión de $U \cap W$ es 1.

8. Ecuaciones cartesianas o implícitas de un subespacio vectorial

Sea U un subespacio vectorial de V. Sea $B = \{\vec{v}_1, \ldots, \vec{v}_n\}$ una base de V, y $B_U = \{\vec{u}_1, \ldots, \vec{u}_r\}$ una base de U. Supongamos que

$$\begin{aligned} \vec{u}_1 &= a_{11}\vec{v}_1 + \cdots + a_{1n}\vec{v}_n, \\ &\vdots \\ \vec{u}_r &= a_{r1}\vec{v}_1 + \cdots + a_{rn}\vec{v}_n. \end{aligned}$$

Sea $\vec{x} = x_1\vec{v}_1 + \cdots + x_n\vec{v}_n$ un vector de V. Recordemos que el vector $\vec{x} \in U$ si y sólo si existen $\lambda_1, \ldots, \lambda r \in K$ tales que

$$\left.\begin{aligned} x_1 &= \lambda_1 a_{11} + \cdots + \lambda_r a_{r1} \\ &\vdots \\ x_n &= \lambda_1 a_{1n} + \cdots + \lambda_r a_{rn} \end{aligned}\right\}.$$

Luego $\vec{x} \in U$ si y sólo si el sistema con incógnitas $\lambda_1, \ldots \lambda_r$

$$\begin{pmatrix} a_{11} & \ldots & a_{r1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{rn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

tiene solución. Y sabemos que equivale a rango $\begin{pmatrix} a_{11} & \ldots & a_{r1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{rn} \end{pmatrix}$ = rango $\begin{pmatrix} a_{11} & \ldots & a_{r1} & x_1 \\ \vdots & \ddots & & \vdots \\ a_{1n} & \ldots & a_{rn} & x_n \end{pmatrix}$.
Esto ocurre cuando unos cuantos determinantes valen cero, proporcionándonos así una sistema de

ecuaciones de la forma

$$\left.\begin{array}{c} b_{11}x_1+\cdots+b_{1n}x_n=0 \\ \vdots \\ b_{k1}x_1+\cdots+b_{kn}x_n=0 \end{array}\right\},$$

a las que llamaremos ecuaciones cartesianas de U respecto de la base B de V.

- Si k es el número de ecuaciones cartesianas independientes que describen a U, entonces $k+\dim(U)=\dim(V)$.

Ejercicio 92: Dada la base $B=\{(1,1,0),(1,0,1),(0,1,1)\}$, calcula las ecuaciones cartesianas respecto de la base B del subespacio vectorial de $\mathbb{R}^3$ generado por $\{(1,2,1)\}$.

Ejercicio 93: Calcula las ecuaciones cartesianas del subespacio vectorial $\langle\{(1,2,3,1),(1,1,1,1),(3,5,7,3)\}\rangle\subseteq\mathbb{Q}^4$.

Ejercicio 94: Consideremos los subespacios vectoriales de $\mathbb{R}^4$, $E_1=\langle\{(1,1,1,1),(1,-1,1,-1)\}\rangle$ y $E_2=\langle\{(1,2,0,2),(1,2,1,2),(3,1,3,1)\}\rangle$.

a) Calcula una base de E_1+E_2.
b) Calcula las ecuaciones cartesianas de E_1+E_2.
c) Calcula las ecuaciones cartesianas de $E_1\cap E_2$.
d) Calcula una base de $E_1\cap E_2$.

Ejercicio 95: Dada la aplicación lineal $f:\mathbb{Z}_5^4\to\mathbb{Z}_5^3$ definida por $f(x,y,z,t)=(x+y,x+z,2x+y+z)$, calcula una base para su núcleo.

maxima 78: Calculemos las ecuaciones cartesianas de $U=\langle\{(1,1,2),(1,-1,0)\}\rangle\subseteq\mathbb{Q}^3$. Sus ecuaciones paramétricas respecto de la base usual son

$$\left.\begin{array}{rl} x= & \lambda+\mu \\ y= & \lambda-\mu \\ z= & 2\lambda \end{array}\right\}.$$

La matriz ampliada de este sistema con incógnitas en los parámetros λ y μ es

```
(%i1) A:matrix([1,1,x],[1,-1,y],[2,0,z]);
```

$$(\%o1)\qquad \begin{pmatrix} 1 & 1 & x \\ 1 & -1 & y \\ 2 & 0 & z \end{pmatrix}$$

Como su rango debe ser dos, su determinante es cero.

```
(%i2) determinant(A);
```

$$(\%o2)\qquad -2z+2y+2x$$

Así la ecuación cartesiana de U es $x+y-z=0$.

Esta ecuación también la podemos encontrar haciendo operaciones elementales por filas en A. Primero extraemos la matriz de coeficientes. Para ello eliminamos la última columna de A.

```
(%i3) C:submatrix(A,3);
```

(%o3) $$\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 2 & 0 \end{pmatrix}$$

Para guardar traza de la operaciones elementales que hacemos en C para obtener su forma triangular reducida, le añadimos al final la matriz identidad.

```
(%i4) M:addcol(C,ident(3));
```

(%o4) $$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ahora triangularizamos y nos quedamos con las últimas columnas, que forman una matriz regular con las operaciones elementales para que C alcance su forma reducida for filas.

```
(%i5) triangularize(M);
```

(%o5) $$\begin{pmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & -2 & 0 & 2 & -1 \\ 0 & 0 & -2 & -2 & 2 \end{pmatrix}$$

```
(%i6) P:submatrix(%,1,2);
```

(%o6) $$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & -1 \\ -2 & -2 & 2 \end{pmatrix}$$

Aplicamos estas operaciones por filas a la matriz inicial y obtenemos en las últimas filas las ecuaciones (en esta caso sólo en la última, pues hay una).

```
(%i7) P.A;
```

(%o7) $$\begin{pmatrix} 2 & 0 & z \\ 0 & -2 & 2y-z \\ 0 & 0 & 2z-2y-2x \end{pmatrix}$$

Si vemos U dentro de $\mathbb{Z}_2^3$, al ser $(1,1,2) = (1,-1,0) = (1,1,0)$, tenemos que las ecuaciones paramétricas ahora son

$$\left.\begin{array}{rcl} x = & \lambda \\ y = & \lambda \\ z = & 0 \end{array}\right\}.$$

Así la matriz ampliada de este sistema es

$$\begin{pmatrix} 1 & x \\ 1 & y \\ 0 & z \end{pmatrix},$$

por lo que una de las ecuaciones, $z = 0$, ya la tenemos. Al ser la dimensión de U uno, necesitamos una ecuación más, que viene de imponer que el determinante de $\begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}$ es cero (el rango de la matriz ampliada es uno), obteniendo $x - y = 0$.

Podemos también utilizar operaciones elementales por filas para llegar a la mismas ecuaciones. En este caso no vamos a utilizar `triangularize`, pues se ve claramente qué operación tenemos que hacer.

```
(%i5) A:matrix([1,x],[1,y],[0,z]);
```

(%o5) $$\begin{pmatrix} 1 & x \\ 1 & y \\ 0 & z \end{pmatrix}$$

```
(%i5) rowop(A,2,1,1);
```

(%o5) $$\begin{pmatrix} 1 & x \\ 0 & y-x \\ 0 & z \end{pmatrix}$$

Obtenemos también que las ecuaciones de U son

$$\left.\begin{matrix} x+y=0 \\ z=0 \end{matrix}\right\}.$$

maxima 79:

Sea U el subespacio de $\mathbb{R}^4$ generado por $\{(1,1,1,1),(1,2,3,1),(1,0,-1,1)\}$. Calculemos sus ecuaciones cartesianas respecto de la base $B=\{(1,1,1,1),(0,1,1,1),(0,0,1,1),(0,0,0,1)\}$.

```
(%i1) modulus:false$
(%i2) A:matrix([1,1,1,1],[1,2,3,1],[1,0,-1,1])$
(%i3) triangularize(A);
```

(%o3) $$\begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

{(1,0,-1,1),(0,2,4,0)} es una base de U. Calculamos ahora las coodenadas de estos vectores respecto de la base B.

```
(%i4) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]
      +t*[0,0,0,1]-[1,0,-1,1], [x,y,z,t]);
```

(%o4) $[[x=1,y=-1,z=-1,t=2]]$

```
(%i5) solve(x*[1,1,1,1]+y*[0,1,1,1]+z*[0,0,1,1]
      +t*[0,0,0,1]-[0,2,4,0], [x,y,z,t]);
```

(%o5) $[[x=0,y=2,z=2,t=-4]]$

```
(%i6) J:matrix([1,-1,-1,2],[0,2,2,-4],[x,y,z,t]);
```

(%o6) $$\begin{pmatrix} 1 & -1 & -1 & 2 \\ 0 & 2 & 2 & -4 \\ x & y & z & t \end{pmatrix}$$

Al exigir que la matriz J tenga rango 2 obtenemos que los siguientes determinantes deben de valer cero.

```
(%i7) determinant(matrix([1,-1,-1],[0,2,2],[x,y,z]));
```

(%o7) $2z-2y$

```
(%i8) determinant(matrix([1,-1,2],[0,2,-4],[x,y,t]));
```

(%o8) $4y+2t$

Las ecuaciones cartesianas de U respecto de B son

$$\left.\begin{matrix} z-y=0 \\ y+t=0 \end{matrix}\right\}.$$

maxima 80:

Sean $U = \{(x,y,z,t) \in \mathbb{Z}_5^4 \mid x+y+z+t = 0,\ x+2t = 0\}$ y $W = \{(x,y,z,t) \in \mathbb{Z}_5^4 \mid 4y+4z+t = 0,\ x+4y = 0\}$. Calculemos una base de la intersección.

```
(%i1)  modulus:5$
(%i2)  M:matrix([1,1,1,1],[1,0,0,2],[0,4,4,1],[1,4,0,0])$
(%i3)  nullspace(M);
```

$$(\%o3) \qquad \operatorname{span}\left(\begin{pmatrix} -2 \\ -2 \\ -2 \\ 1 \end{pmatrix}\right)$$

Una base es de la intersección es $\{(3,3,3,1)\}$.

maxima 81:

Sea $f : \mathbb{Q}^4 \to \mathbb{Q}^3$, $f(x,y,z,t) = (x+y, z+t, x+y+z+t)$. Calculemos una base de $N(f)$.

```
(%i1)  modulus:false4
(%i2)  N:matrix([1,1,0,0],[0,0,1,1],[1,1,1,1])$
(%i3)  nullspace(N);
```

$$(\%o3) \qquad \operatorname{span}\left(\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}\right)$$

Por tanto una base de $N(f)$ es $\{(-1,1,0,0),(0,0,1,-1)\}$.

Capítulo 9

Diagonalización de matrices. Forma normal de Jordan

Contenidos de este capítulo

1. Matrices diagonalizables

Una matriz diagonal es una matriz cuadrada que tiene todas sus entradas nulas, salvo eventualmente las de la diagonal. Una matriz cuadrada A es diagonalizable si existen una matriz diagonal D y una matriz regular P tales que $A = PDP^{-1}$.

La diagonalización de matrices es útil para el cálculo de potencias grandes de una matriz, ya que

$$A^r = (PDP^{-1})^r = PDP^{-1}PDP^{-1} \overset{r-1}{\cdots} PDP^{-1} = PD^rP^{-1}.$$

En adelante, A representará una matriz cuadrada de orden $n \times n$ sobre un cuerpo K.

Un elemento $\lambda \in K$ es un valor propio de A si existe $x \in K^n \setminus \{(0,\dots,0)\}$ tal que $Ax = \lambda x$. En tal caso diremos que x es un vector propio asociado al valor propio λ.

Teorema de caracterización de los valores propios. Un elemento $\lambda \in K$ es un valor propio de A si y sólo si $|A - \lambda I_n| = 0$.

Así los valores propios de A son las raíces del polinomio $|A - \lambda I_n| \in K[\lambda]$, que se conoce como polinomio característico de A, y lo denotaremos por $p_A(\lambda)$. Nótese que $gr(p_A(\lambda) = n$.

Ejercicio 96: Calcula el polinomio característico y los valores propios de $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Propiedades.

1) Si A es una matriz triangular, entonces sus valores propios son los valores de la diagonal.
2) Los valores propios de A y A^t coinciden.
3) $|A| = 0$ si y sólo si 0 es un valor propio de A.
4) Si A es regular y λ es un valor propio de A, entonces λ^{-1} lo es de A^{-1}.

- Si λ es un valor propio de A, entonces

$$V(\lambda) = \{x \in K^n \text{ tales que } (A - \lambda I_n)x = 0\},$$

(en este caso $0 = (0,\dots,0) \in K^n$) es un subespacio vectorial de K^n. Dicho subespacio lo llamamos subespacio vectorial propio asociado al valor propio λ.

Ejercicio 97: Encuentra los subespacios propios asociados a los valores propios de $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Sean $\lambda_1, \ldots, \lambda_k$ los valores propios de la matriz A. A la multiplicidad de la raíz λ_i de $P_A(\lambda)$ la llamaremos multiplicidad algebraica de λ_i, mientras que la dimensión de $V(\lambda_i)$ es la multiplicidad geométrica de λ_i.

Ejercicio 98: Calcula las multiplicidades algebraicas y geométricas de los valores propios de $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

- La multiplicidad geométrica de un valor propio es menor o igual que su multiplicidad algebraica.

Criterio de diagonalización. A es diagonalizable si, y sólo si, la suma de las multiplicidades algebraicas de los valores propios de A es n y además para todo valor propio las multiplicidades algebraica y geométrica coinciden.

- Toda matriz cuadrada y simétrica con coeficientes en $\mathbb{R}$ es diagonalizable.

2. Método para diagonalizar una matriz

1) Calculamos $p_A(\lambda)$, sus raíces $\lambda_1, \ldots, \lambda_k$ y sus multiplicidades algebraicas, $m_1, \ldots, m_k$.
2) Si $m_1 + \cdots + m_k \neq n$, A no es diagonalizable.
3) En caso contrario, para cada λ_i, calculamos el subespacio propio $V(\lambda_i)$ y su dimensión. Si dicha dimensión no coincide con m_i para algún i, entonces A no es diagonalizable.
4) Llegado este paso, la matriz A es diagonalizable y D es la matriz que tiene en la diagonal m_1 entradas λ_1, m_2 entradas λ_2, y así hasta m_k entradas λ_k. La matriz de paso P se construye colocando en las primeras m_1 columnas una base de $V(\lambda_1)$, a continuación en las siguientes m_2 columnas una base de $V(\lambda_2)$, y así hasta que colocamos en las últimas m_k columnas una base de $V(\lambda_k)$.

Ejercicio 99: Diagonaliza la matriz $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Ejercicio 100: Diagonaliza la matriz

$$\begin{pmatrix} 2 & 0 & 0 \\ -15 & -4 & 3 \\ -35 & -14 & 9 \end{pmatrix} \in \mathcal{M}_{3\times 3}(\mathbb{R}).$$

Ejercicio 101: Demuestra que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ con coeficientes reales no es diagonalizable.

maxima 82: Sea

```
(%i1) A:matrix([-1,3,3],[0,2,0],[3,-3,-1]);
```

(%o1)
$$\begin{pmatrix} -1 & 3 & 3 \\ 0 & 2 & 0 \\ 3 & -3 & -1 \end{pmatrix}$$

El comando `eigenvectors` nos proporciona toda la información para saber si es diagonalizable.

```
(%i2) eigenvectors(A);
```

(%o2) $$[[[-4,2],[1,2]],[[[1,0,-1]],[[1,0,1],[0,1,-1]]]]$$

La salida nos dice que los valores propios son -4 y 2, con multiplicidades 1 y 2, respectivamente. Además nos da bases para $V(-4), \{(1,0,-1)\}$ y $V(2), \{(1,0,1),(0,1,-1)\}$. Como las multiplicidades algebraicas y geométricas coinciden, y suman 3, A es diagonalizable.

La matriz de paso se calcula poniendo dichas bases una a continuación de la otra en columnas.

```
(%i3) P:matrix([1,1,0],[0,0,1],[-1,1,-1]);
```

(%o3) $$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix}$$

Comprobamos que efectivamente están bien hechos los cálculos:

```
(%i4) P^^(-1).A.P;
```

(%o4) $$\begin{pmatrix} -4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Podríamos también haber hecho los cálculos paso a paso, calculando primero el polinomio característico de A.

```
(%i5) charpoly(A,x);
```

(%o5) $$(-x-1)^2\,(2-x)-9\,(2-x)$$

Para ver los valores propios, lo factorizamos.

```
(%i6) factor(%);
```

(%o6) $$-(x-2)^2\,(x+4)$$

Y para calcular una base de por ejemplo $V(2)$ utilizamos `nullspace`.

```
(%i7) nullspace(A-2*ident(3));
```

(%o7) $$\mathrm{span}\left(\begin{pmatrix} -3 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix}\right)$$

3. Forma normal de Jordan

maxima 83: Vamos a estudiar si la siguiente matriz es o no diagonalizable.

```
(%i1) A:matrix([3,1,1],[-1,5,1],[0,0,4]);
```

(%o1) $$\begin{pmatrix} 3 & 1 & 1 \\ -1 & 5 & 1 \\ 0 & 0 & 4 \end{pmatrix}$$

Llamamos I a la identidad, que vamos a necesitar luego.

```
(%i2) I:ident(3);
```

(%o2) $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

El polinomio característico de A es

```
(%i3)  factor(charpoly(A,x));
```
$$(\%o3)\quad -(x-4)^3$$

Por lo que sólo hay un valor propio, con multiplicidad algebraica 3.

```
(%i4)  eigenvectors(A);
```
$$(\%o4)\quad [[[4],[3]],[[[1,0,1],[0,1,-1]]]]$$

Como vemos, sólo hay dos vectores en el subespacio propio $V(4)$, el núcleo de $A-4I$, por lo que A no es diagonalizable. Sin embargo el núcleo de $(A-4I)^2$ sí que tiene dimensión tres.

```
(%i5)  nullspace((A-4*I)^^2);
```
$$(\%o5)\quad \text{span}\left(\begin{pmatrix}0\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\end{pmatrix}\right)$$

Tomemos uno de ellos que no esté en $V(4)$. Al multiplicarlo por $(A-4I)$ nos saldrá un elemento de $V(4)$, que además es linealmente independiente con el elemento original.

```
(%i6)  (A-4*I).[1,0,0];
```
$$(\%o6)\quad \begin{pmatrix}-1\\-1\\0\end{pmatrix}$$
```
(%i7)  (A-4*I).%;
```
$$(\%o7)\quad \begin{pmatrix}0\\0\\0\end{pmatrix}$$

Tenemos así dos elementos linealmente independientes de $\mathbb{Q}^3$, uno de ellos en $V(4)$. Como quiera que $V(4)$ tiene dimensión dos, podemos aún elegir otro elemento de $V(4)$ que sea linealmente independiente con éste. Ponemos estos tres vectores en una matriz (que será invertible al ser linealmente independientes).

```
(%i8)  P:transpose(matrix([1,0,1],[-1,-1,0],[1,0,0]))$
```
Y obtenemos que aunque A no sea diagonalizable, se acerca bastante a serlo.

```
(%i9)  P^^(-1).A.P;
```
$$(\%o9)\quad \begin{pmatrix}4&0&0\\0&4&1\\0&0&4\end{pmatrix}$$

maxima 84: Consideremos ahora la matriz con coeficientes racionales

```
(%i1)  A:matrix([4,2,0,0],[0,6,2,0],[1,-1,7,-1],[-1,1,-1,5]);
```
$$(\%o1)\quad \begin{pmatrix}4&2&0&0\\0&6&2&0\\1&-1&7&-1\\-1&1&-1&5\end{pmatrix}$$
```
(%i2)  I:ident(4)$
```
El polinomio característico de A factoriza como

```
(%i3)  factor(charpoly(A,x));
```
$$(\%o3)\quad (x-6)^3\,(x-4)$$

Por lo que tenemos dos valores propios: 4 y 6, de multiplicidades algebraicas 1 y 4, respectivamente.

```
(%i4)  eigenvectors(A);
```
(%o4) $[[[6,4],[3,1]],[[[1,1,0,0]],[[1,0,0,1]]]]$

Esto nos dice que el núcleo de $A-6I$ tiene dimensión 1 (y está generado por $(1,1,0,0)$) por lo que nos hacen falta dos vectores más para completar la multiplicidad algebraica. Para $A-4I$, la dimensión de su núcleo es 1, que coincide con la multiplicidad algebraica de 4. Por ello ya tenemos un candidato para la matriz de paso, el $(1,0,0,1)$ (y otro será $(1,1,0,0)$ o un múltiplo suyo).

Veamos qué ocurre con los núcleos de las potencias de $A-6I$.

```
(%i5)  nullspace((A-6*I)^^2);
```
(%o5) $\text{span}\left(\begin{pmatrix}0\\8\\8\\0\end{pmatrix},\begin{pmatrix}8\\0\\-8\\0\end{pmatrix}\right)$

La dimensión de éste es dos, por lo que seguimos intentando con $(A-6I)^3$.

```
(%i6)  nullspace((A-6*I)^^3);
```
(%o6) $\text{span}\left(\begin{pmatrix}-4\\-4\\0\\0\end{pmatrix},\begin{pmatrix}0\\-4\\-4\\0\end{pmatrix},\begin{pmatrix}0\\0\\4\\-4\end{pmatrix}\right)$

Cuya dimensión llena completamente la multiplicidad algebraica de 6. Escogemos un vector que esté en el núcleo de $(A-6I)^3$ pero que no esté en el núcleo de $(A-6I)^2$, y calculamos la secuencia que resulta de ir multiplicando por $A-6I$ hasta que lleguemos a $V(6)$.

```
(%i7)  (A-6*I).[0,0,1,-1];
```
(%o7) $\begin{pmatrix}0\\2\\2\\0\end{pmatrix}$

```
(%i8)  (A-6*I).%;
```
(%o8) $\begin{pmatrix}4\\4\\0\\0\end{pmatrix}$

```
(%i9)  (A-6*I).%;
```
(%o9) $\begin{pmatrix}0\\0\\0\\0\end{pmatrix}$

Como hemos conseguido tres nuevos vectores linealmente independientes, y teníamos ya uno de $V(4)$, no tenemos que seguir buscando más. Así, escogiendo como matriz de paso:

```
(%i10) P:transpose(matrix([1,0,0,1],[4,4,0,0],[0,2,2,0],[0,0,1,-1]))$
```

Obtenemos que A se puede expresar en la base cuyos elementos son las columnas de P de la siguiente forma.

```
(%i11) P^^(-1).A.P;
```

$$(\%o11)\quad \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 6 & 1 & 0 \\ 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

Las matrices de los dos últimos ejemplos no eran diagonalizables, sin embargo hemos encontrado bases respecto de las cuales tienen en la diagonal sus valores propios (repetidos tantas veces como sus respectivas multiplicidades algebraicas), y eventualmente tienen algún 1 encima de alguna posición en la diagonal. De hecho el número de unos viene a medir lo lejos que están de ser diagonalizables. Los dos ejemplos se han desarrollando siguiendo las siguientes ideas.

Subespacios propios generalizados. Sea A una matriz cuadrada de orden n con coeficientes en $\mathbb{C}$ (así nos aseguramos que el polinomio característico descompone totalmente como producto de polinomios de grado uno, y la suma de las multiplicidades algebraicas es precisamente n). Sea λ un valor propio de A. Consideremos los subespacios de $\mathbb{C}^n$. Definimos

$$V_i(\lambda) = N((A - \lambda Id)^i),$$

el i-ésimo subespacio propio generalizado asociado a λ.

Se tiene trivialmente que $V(\lambda) = V_1(\lambda) \subseteq V_2(\lambda) \subseteq \cdots$. Como todos esos conjuntos son subespacios de $\mathbb{C}^n$, sabemos que esa cadena se volverá estacionaria, alcanzando el mayor subespacio posible, en un número finito de pasos. Es fácil comprobar que si $V_i(\lambda) = V_{i+1}(\lambda)$, entonces $V_i(\lambda) = V_j(\lambda)$ para todo entero j mayor o igual que i. Por tanto, nos aseguramos que el subespacio más grande posible es $V_n(\lambda)$. Se tiene además que para un i como el anterior, entonces $\dim(V_i(\lambda))$ (y por tanto $\dim(V_n(\lambda))$) es precisamente la multiplicidad algebraica de λ, y el subspacio $V_i(\lambda)$ es invariante por A, a saber, para cualquier $v \in V_i(\lambda)$, Av vuelve a estar en $V_i(\lambda)$.

De esta forma, si $\lambda_1, \ldots, \lambda_k$ son los distintos valores propios de A con multiplicidades $m_1, \ldots, m_k$, respectivamente (recordemos que $m_1 + \cdots + m_k = n$ en nuestro caso), si elegimos B_i una base para cada $V_n(\lambda_i)$, entonces la matriz A respecto de esa base tiene el siguiente aspecto

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_k \end{pmatrix}$$

donde cada matriz A_i es cuadrada de orden m_i, y el resto de las entradas son todas 0. En el caso en que A sea diagonalizable $V(\lambda_i) = V_n(\lambda_i)$, y podemos conseguir que A_i sea una matriz diagonal cuyos valores de la diagonal son todos λ_i.

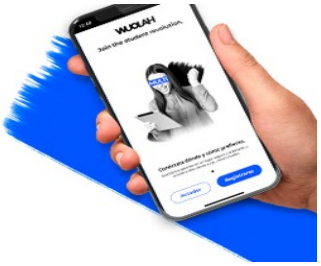
Orden de un elemento de un subespacio propio generalizado. Decimos que un vector v de $V_n(\lambda)$, con λ un valor propio de A, es de orden v si $v \in V_k(\lambda) \setminus V_{k-1}(\lambda)$ (a saber, $(A - \lambda Id)^k v = 0$ y $(A - \lambda Id)^{k-1} v \neq 0$).

Bloque de Jordan. Sea $v \in V_k(\lambda) \setminus V_{k-1}(\lambda)$. Entonces los vectores

$$v_k = v, v_{k-1} = (A - \lambda Id)v, \ldots, v_1 = (A - \lambda)^{k-1} v \tag{1}$$

son linealmente independientes. Es más, como

$$Av_k = v_{k-1} + \lambda v_k, \ldots,\ Av_i = v_{i-1} + \lambda v_i, \ldots,\ Av_2 = v_1 + \lambda v_2,\ Av_1 = \lambda v_1,$$



se tiene que el subespacio U generado por $\{v_1, \ldots, v_k\}$ es invariante por A, y la expresión de la aplicación lineal asociada a A restringida a U respecto de la base $\{v_1, \ldots, v_k\}$ es de la forma

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & 0 & \lambda & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{pmatrix},$$

al que llamaremos bloque de Jordan de tamaño k asociado a λ.

Si para cada $V_n(\lambda_i)$ buscamos un elemento de orden máximo y calculamos la secuencia asociada a éste como en (1), obtendremos parte de una base de $V_n(\lambda)$. Si el número de elementos de la secuencia no es igual a m_i, entonces buscamos de nuevo otro elemento de orden máximo que no esté en el espacio generado por los que ya hemos calculado anteriormente y le calculamos su secuencia asociada (1). Siguiendo este proceso acabaremos por llenar m_i elementos en la base, y tendremos así que A_i respecto de esa base está formada por una matriz diagonal en bloques, y en la diagonal aparecerán bloques de Jordan de tamaño las longitudes de las secuencias que hemos ido considerando. Cuando juntemos todas las bases que hemos obtenido para cada $V_n(\lambda_i)$ llegaremos a que la matriz A se puede expresar en esa base como una matriz en diagonal por bloques, y esos bloques son bloques de Jordan asociados a los valores propios de A, y que tienen tamaño las longitudes de las secuencias (1) utilizadas para construir las distintas bases de los subespacios propios generalizados. La matriz resultante se conoce como forma de Jordan asociada a A y es única salvo reordenamiento de los bloques.